Izabela Oleksiewicz

OCHRONA CYBERPRZESTRZENI UNII EUROPEJSKIEJ

POLITYKA ▪ STRATEGIA ▪ PRAWO

PWN

OCHRONA CYBERPRZESTRZENI UNII EUROPEJSKIEJ

Izabela Oleksiewicz

OCHRONA CYBERPRZESTRZENI UNII EUROPEJSKIEJ

POLITYKA ▪ STRATEGIA ▪ PRAWO

PWN

Projekt okładki **Joanna Andryjowicz**

Wydawca **Wioleta Szczygielska-Dybciak**

Redaktor **Jolanta Kucharska**

Koordynator produkcji **Anna Bączkowska**

Skład wersji elektronicznej na zlecenie Wydawnictwo Naukowe PWN
Michał Latusek

Recenzenci
prof. dr hab. Stanisław Koziej, Uczelnia Łazarskiego
dr hab. Piotr Dela, profesor Akademii Sztuki Wojennej
dr hab. Agnieszka Bógdał-Brzezińska, Uniwersytet Warszawski

Zastrzeżonych nazw firm i produktów użyto w książce wyłącznie w celu identyfikacji.

Copyright © by Wydawnictwo Naukowe PWN SA
Warszawa 2021

ISBN 978-83-01-21764-8

eBook został przygotowany na podstawie wydania papierowego z 2021r. (Wydanie I)
Warszawa 2021

Wydawnictwo Naukowe PWN SA
02-460 Warszawa, ul. Gottlieba Daimlera 2
tel. 22 69 54 321, faks 22 69 54 288
infolinia 801 33 33 88
e-mail: pwn@pwn.com.pl, reklama@pwn.pl
www.pwn.pl

SPIS TREŚCI

Wykaz skrótów

Wstęp

1. Geneza i istota bezpieczeństwa informacyjnego

1.1. Geneza bezpieczeństwa informacyjnego w Unii Europejskiej

1.2. Istota bezpieczeństwa informacyjnego w Unii Europejskiej

2. Strategia cyberbezpieczeństwa Unii Europejskiej w XXI w.

2.1. Paradygmat bezpieczeństwa państwa w stosunkach międzynarodowych

2.2. Europejska strategia bezpieczeństwa jako instrument polityki cyberbezpieczeństwa Unii Europejskiej

2.3. Istota strategii ochrony cyberprzestrzeni Unii Europejskiej

3. Uwarunkowania cyberbezpieczeństwa Unii Europejskiej

3.1. Istota i zakres cyberterroryzmu jako zagrożenia w XXI w.

3.2. Uwarunkowania zagrożeń cyberterrorystycznych w Unii Europejskiej

3.2.1. Uwarunkowania zewnętrzne

3.2.2. Uwarunkowania wewnętrzne

4. Prawne standardy cyberbezpieczeństwa Unii Europejskiej

4.1. Międzynarodowe normy prawne w zakresie zwalczania cyberterroryzmu

4.1.1. Rada Europy wobec cyberprzestępczości

4.1.2. Interpol w walce z cyberterroryzmem

4.1.3. Organizacja Narodów Zjednoczonych w walce z cyberterroryzmem

4.2. Prawo unijne wobec cyberterroryzmu

4.2.1. Prawo pierwotne Unii Europejskiej wobec cyberterroryzmu

4.2.1.1. Traktat z Maastricht

4.2.1.2. Traktat z Amsterdamu

4.2.1.3. Traktat z Nicei

4.2.1.4. Traktat z Lizbony

4.2.2. Prawo wtórne Unii Europejskiej wobec cyberterroryzmu

4.2.3. Instytucjonalny wymiar zwalczania cyberprzestępczości w prawie Unii Europejskiej

5. Realizacja polityki cyberbezpieczeństwa Unii Europejskiej

5.1. Unia jako podmiot polityki ochrony cyberbezpieczeństwa

5.2. Instrumenty polityki cyberbezpieczeństwa

5.2.1. Europol i SIS

5.2.2. Eurojust

5.2.3. Agencja UE ds. Cyberbezpieczeństwa (Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji)

5.2.4. Europejskie Centrum ds. Walki z Cyberprzestępczością

5.2.5. Decyzje ramowe i strategie UE dotyczące problematyki zwalczania cyberterroryzmu

6. Implementacja polityki cyberbezpieczeństwa w Unii Europejskiej na przykładzie wybranych państw

6.1. Implementacja polityki cyberbezpieczeństwa w Estonii

6.1.1. Podstawowe dokumenty w zakresie polityki cyberbezpieczeństwa

6.1.2. Instytucjonalny wymiar polityki cyberbezpieczeństwa

6.2. Implementacja polityki cyberbezpieczeństwa w Polsce

6.2.1. Podstawowe dokumenty w zakresie polityki cyberbezpieczeństwa

6.2.2. Polski Kodeks karny wobec polityki cyberbezpieczeństwa

6.2.3. Wymiar instytucjonalny zwalczania cyberterroryzmu w Polsce

6.2.4. Dyrektywa NIS w prawie polskim

6.3. Implementacja polityki cyberbezpieczeństwa w RFN

6.3.1. Podstawa prawna polityki cyberbezpieczeństwa

6.3.2. Instytucjonalny wymiar polityki cyberbezpieczeństwa RFN

6.4. Implementacja polityki cyberbezpieczeństwa we Francji

6.4.1. Podstawowe dokumenty w zakresie polityki cyberbezpieczeństwa

6.4.2. Instytucjonalny wymiar polityki cyberbezpieczeństwa

6.5. Implementacja polityki cyberbezpieczeństwa w Wielkiej Brytanii

6.5.1. Podstawowe dokumenty w zakresie polityki cyberbezpieczeństwa

6.5.2. Instytucjonalny wymiar polityki cyberbezpieczeństwa

7. Skutki i perspektywy rozwoju strategii i polityki cyberbezpieczeństwa Unii Europejskiej

7.1. Skutki polityki i strategii cyberbezpieczeństwa Unii Europejskiej

7.2. Perspektywy polityki i strategii cyberbezpieczeństwa Unii Europejskiej

Zakończenie

Bibliografia

O Autorce

Przypisy

WYKAZ SKRÓTÓW

ANSSI	– Agence Nationale De La Sécurité Des Systèmes d'Information (Krajowa Agencja Bezpieczeństwa Systemów Informacyjnych)
CATS	– Coordinating Committee in the area of police and judicial cooperation in criminal matters (Komitet Koordynacyjny w dziedzinie Współpracy Policji i Wymiarów Sprawiedliwości w Sprawach Karnych)
CERT	– Computer Emergency Response Team (Zespół Reagowania na Incydenty Komputerowe)
CNSA	– Contact Network of Spam Enforcement Authorities
CODE	– Forschungszentrum Cyber Operational Defense (Centrum Badań Cyberobrony)
COREPER	– Comité des représentants permanents (Komitet Stałych Przedstawicieli)
CSIRT	– Computer Security Incident Response Team (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego)
DCRG	– Direction Centrale des Renseignements (Centralna Dyrekcja Wywiadu Ogólnego)
DCRI	– Centralna Dyrekcja Wywiadu Krajowego
DCPJ	– Centrale de la Police Judiciaire (Centralna Dyrekcja Policji Sądowej)
DDoS	– atak na system koputerowy (Distributed Denial of Service)
DGPN	– Direction Générale de la Police Nationale (Dyrekcja Generalna Policji Narodowej)

DNAT	– Division Nationale Antiterroriste (Narodowy Wydział Antyterrorystyczny)
DST	– Direction de la Surveillance du Territoire
Dyrektywa NIS	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w *sprawie* środków na rzecz wysokiego wspólnego poziomu *bezpieczeństwa sieci* i *systemów informatycznych* na terytorium Unii Europejskiej
RODO	– Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (*General Data Protection Regulation – GDPR)*
EC3	– European Cybercrime Centre (Europejskie Centrum ds. Walki z Cyberprzestępczością)
EIK	– Europejska Infrastruktura Krytyczna
ENA	– Europejski nakaz aresztowania
END	– Europejski nakaz dochodzeniowy
ENISA	– The European Union Agency for Cybersecurity (Agencja ds. Bezpieczeństwa Cybernetycznego Unii Europejskiej)
ESB	– Europejska strategia bezpieczeństwa
ETS	– Europejski Trybunał Sprawiedliwości
Eurojust	– European Union Agency for Criminal Justice Cooperation (Europejska Jednostka Współpracy Sądowej)
Europol	– European Union Agency for Law Enforcement Cooperation (Agencja Unii Europejskiej ds. Współpracy Organów Ścigania)
G-7	– *Grupa G-7 (Group of Seven)*
ICT	– Information and Communication Technology (Technologia informacyjna i komunikacyjna)

IGCI – Interpol Global Complex for Innovation (Globalny Zespół Innowacji Interpolu)

INTERPOL – The International Criminal Police Organization (Międzynarodowa Organizacja Policji Kryminalnej)

ITIF – Information Technology and Innovation Foundation (Fundacja na rzecz Technologii Informacyjnej i Innowacyjności)

JHA Council – Justice and Home Affairs Council (Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych – Rada WSiSW)

KE – Komisja Europejska

LIBE – Committee on Civil Liberties, Justice and Home Affairs (Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych)

NATO – pakt północnoatlantycki

ODPU – ustawa o ochronie danych osobowych z dnia 10.05.2018 r.

OECD – The Organisation for Economic Co-operation and Development (Organizacja Współpracy Gospodarczej i Rozwoju)

ONZ – Organizacja Narodów Zjednoczonych

PE – Parlament Europejski

PPK – Pojedynczy Punkt Kontaktowy

RODO – *Rozporządzenie o ochronie danych osobowych (*General Data Protection Regulation – GDPR)

SBZ – Strategia bezpieczeństwa zewnętrznego

SIS – System Informacyjny Schengen (Schengen Information System)

SIS – brytyjska służba specjalna powołana w 1909 r. do prowadzenia wywiadu zagranicznego (Secret Intelligence Service, MI6)

TA – Traktat amsterdamski (Traktat z Amsterdamu zmieniający Traktat o Unii Europejskiej, Traktaty

	ustanawiające Wspólnoty Europejskie oraz niektóre związane z nimi akty)
TFUE	– Traktat o funkcjonowaniu Unii Europejskiej
TL	– Traktat lizboński (Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską)
TM	– Traktat z Maastricht
TN	– Traktat z Nicei
TUE	– Traktat o Unii Europejskiej
TWE	– Traktat Wspólnot Europejskich
UE	– Unia Europejska
UCLAT	– Unité de Coordination de la Lutte Antiterroriste (Jednostka Koordynująca Walkę z Terroryzmem)
UZE	– Unia Zachodnioeuropejska
WPBiO	– Wspólna Polityka Bezpieczeństwa i Obrony UE
WPT	– Rada Grupy Roboczej ds. Terroryzmu
WSiSW	– Wymiar Sprawiedliwości i Spraw Wewnętrznych (Justice and Home Affairs – JHA)
EJN	– Europejska Sieć Sądowa
UNODC	– United Nations Office on Drugs and Crime
UNICITRAL	– United Nation Commission on International Trade Law
RE	– Rada Europy
OECD	– Organizacja Współpracy Gospodarczej i Rozwoju
VIS	– Visa Information System (Wizowy System Informacyjny)

WSTĘP

Jesteśmy niewolnikami prawa, abyśmy mogli być wolni.
Cyceron

Informacja jest elementarnym składnikiem wszelkich przedsięwzięć. Jej posiadanie pozwala na stworzenie zasobów informacji, które stają się podstawą lepszych i bezpieczniejszych warunków życia. W XXI wieku informacja zyskuje coraz większą wartość i znaczenie. Rozwój technologii informacyjnych oraz powstanie i rozwój społeczeństwa opartego na wiedzy prowadzi do pojawienia się nowych zagrożeń dla jego funkcjonowania. Przy obecnym stopniu uzależnienia wszystkich obszarów życia i działalności człowieka od informacji brak dostępu do niej może zaburzyć właściwe działanie systemów teleinformatycznych i prowadzić do utraty bezpieczeństwa. Zadaniem bezpieczeństwa informacyjnego jest zatem dążenie do wykluczenia wszelkich zagrożeń w tej kwestii.

Bez dysponowania informacją o sytuacji trudno podjąć działania zmierzające do osiągnięcia celu. Droga, jaką przebywa informacja od nadawcy do adresata, umożliwia ocenę potencjału jej ochrony. Takie zdolności ochronne nie są tylko konsekwencją uwarunkowań technicznych i technologicznych środków teleinformatycznych, lecz także w dużej mierze zależą od odbiorcy, do którego przekaz jest kierowany. Odbiorem informacji i jej dalszym rozpowszechnianiem zawsze zajmuje się człowiek, który może ją wykorzystać niezgodnie z intencjami autora. Powszechnie wiadomo, że najsłabszym ogniwem bezpieczeństwa jest człowiek i to głównie od niego będzie zależało bezpieczeństwo informacji. Dzięki powstaniu i szybkiemu rozwojowi Internetu użytkownicy nie mają ograniczeń dostępu do zbiorów danych na całym świecie. Zmagania z dostępem do nich na

płaszczyźnie wojskowej, technologicznej, przemysłowej i finansowej są jednym z najważniejszych interesów państwa i społeczeństwa informacyjnego[1].

Pojęcie bezpieczeństwa od wiek wieków było wysoko cenione. Takie słowa jak: pokój, spokój i szczęście wyrażały poczucie bezpieczeństwa i stały się jego wyznacznikiem. Bezpieczeństwo nie jest stanem jednorodnym, nie jest również jednoznacznie sprecyzowanym celem człowieka i społeczeństw. Obejmuje różne zakresy działania i jest zjawiskiem bardzo złożonym. Dotyczy wielu obszarów, w tym społecznego, politycznego, militarnego, ekonomicznego, kulturowego i prawnego. Można jednak wskazać wspólny mianownik, który łączy bezpieczeństwo z „poczuciem stabilności i trwałości określonego stanu rzeczy, z odczuciem braku zagrożenia wewnętrznego lub zewnętrznego, a także z doznawaniem pewności i spokoju w codziennym bytowaniu, ufności i zaufania do przyszłości”[2].

Stanowiąc element bezpieczeństwa, informacja zawsze miała znaczenie i była doceniana przez władców, przywódców, wodzów i dowódców. Odgrywała istotną rolę podczas podejmowania ważnych strategicznie decyzji. Miała także zasadnicze znaczenie w gospodarce i zdobywaniu wiedzy o rynkach finansowych. Termin „bezpieczeństwo informacyjne” został rozpowszechniony dopiero w drugiej połowie XX wieku. Prawdziwej rewolucji dokonał Internet, który stał się niezbędnym narzędziem zapewniającym wymianę informacji na niespotykaną skalę. Szybki i łatwy dostęp do niej, nieograniczony czasowo i geograficznie, to tylko niektóre korzyści wynikające z funkcjonowania w sieci. Niestety niesie to również nowe zagrożenia dotyczące bezpieczeństwa informacji, systemów teleinformacyjnych oraz prywatności. Bezpieczne funkcjonowanie w cyberprzestrzeni wymusza konieczność zapewnienia zasobom informacji w systemach teleinformatycznych odpowiednich, niezagrożonych działań podczas ich gromadzenia, przetwarzania, przechowywania i przesyłania[3].

Informacja jest zasobem, a każdy obszar działalności człowieka i państwa staje się coraz częściej zależny od dostarczenia informacji i

funkcjonowania systemów opartych na informacjach. Wojsko, gospodarka, energetyka, media, systemy bankowe i komunikacyjne są w dużym stopniu oparte na systemach informacyjnych. Odgrywają one główną rolę w procesie podejmowania decyzji w organizacjach cywilnych i wojskowych. W związku z tym coraz większego znaczenia nabiera „pozytywne" ujęcie bezpieczeństwa informacyjnego w odróżnieniu od tradycyjnego „negatywnego" jako stanu wolnego od zagrożeń[4].

Celem tego opracowania jest analiza działań podjętych w polityce ochrony cyberprzestrzeni przez Unię Europejską (UE) jako obowiązku zabezpieczenia wspólnej przestrzeni bezpieczeństwa informacyjnego UE w obliczu współczesnych zagrożeń. Zostanie również dokonana analiza aktualnej strategii cyberbezpieczeństwa, polityki i regulacji w wymiarze instytucjonalno-prawnym w odniesieniu do standardów międzynarodowych i unijnych, w kierunku ustanowienia reguł współpracy między Unią a państwami członkowskimi.

Głównym problemem badawczym jest wykazanie, jak istotnym elementem bezpieczeństwa Unii Europejskiej jest umiejętnie prowadzona polityka i strategia cyberbezpieczeństwa na poziomie zarówno unijnym, jak i poszczególnych państw członkowskich. Ma to istotne znaczenie dla bezpieczeństwa wewnętrznego tych państw oraz całej UE. Została też podjęta próba wykazania, że to współpraca na poziomie państw członkowskich oraz na poziomie międzyinstytucjonalnym w konkretnych krajach ma zasadnicze znaczenie dla skuteczności zwalczania zjawiska cyberterroryzmu.

W obliczu rosnących zagrożeń informacyjnych wraz ze złożonością problemów występujących w tym obszarze strategia narodowa i cyberstategia, dotyczące ochrony cyberprzestrzeni, pełnią niezwykle istotną funkcję dla bezpieczeństwa zewnętrznego państwa, a także przyczyniają się do wzrostu bezpieczeństwa całej Unii. W tej publikacji zostanie wykazane, że nieścisłości prawne i rozbieżności regulacyjne na poziomie unijnym, dotyczące podziału kompetencji odnoszących się do ochrony cyberprzestrzeni,

prowadzą do opóźnienia nawiązania współpracy między Unią a państwami członkowskimi.

Impulsem do podjęcia takich działań okazały się głębokie procesy transformacyjne związane z rewolucją przemysłową 4.0 zainicjowaną przez Niemcy, a następnie technologią 5G[5]. Zbliżające się zmiany cywilizacyjne są dla poszczególnych społeczeństw sprawdzianem zdolności uczenia się i od tego, jak rozpoznają one i wykorzystają pojawiające się szanse oraz jak poradzą sobie z zagrożeniami, będzie zależał porządek i układ sił na świecie. Wśród największych wyzwań dla społeczeństwa 5.0 wymienia się związane z zapewnieniem powszechnego bezpieczeństwa na świecie zmieniającym się w sposób nieoczekiwany pod wpływem cyfryzacji i rewolucji sieciowej. Od zdolności wczesnego rozpoznania cyberzagrożeń i radzenia sobie z wyzwaniami cyberbezpieczeństwa będą zależeć wszystkie istotne dziedziny życia społecznego i jednostkowego: bezpieczeństwo państwa, obronność, demokracja, ład prawny, swobody obywatelskie, rozwój gospodarczy i powszechny dobrobyt, a także więzi międzyludzkie i zadowolenie z życia. Fundamentalnym warunkiem właściwego przygotowania się na wyzwania przyszłości odnoszące się do cyberbezpieczeństwa są rozwój i upowszechnienie odpowiednich kompetencji kluczowych z punktu widzenia cyberbezpieczeństwa przez właściwie programowane procesy edukacyjne, w tym zwłaszcza procesy w obszarze szkolnictwa wyższego.

Podmiotem analizy badawczej jest Unia Europejska, a jej przedmiotem ochrona cyberbezpieczeństwa podejmowana w ramach polityki, strategii i prawa na poziomie zarówno UE, jak i państwowym w związku ze zwalczaniem zagrożenia cyberterroryzmem. Analiza instytucjonalno-prawna ochrony cyberprzestrzeni w wybranych państwach Unii pozwoli wskazać sposoby oraz różną efektywność i szczegółowość uregulowania tej samej problematyki na szczeblu państwowym, będąc członkiem UE i jednocześnie stroną tych samych konwencji międzynarodowych. Autorka zdecydowała się poddać szczegółowej analizie przykłady Niemiec, Francji i Wielkiej Brytanii jako wiodących aktorów w

ochronie cyberprzestrzeni w Europie. Wybór Estonii i Polski został podyktowany faktem, że są to państwa tzw. nowej Unii, Estonia natomiast po wydarzeniach z 2007 r. posiada obecnie jeden z bardziej rozwiniętych systemów prewencji w cyberprzestrzeni. Z kolei od niedawna wdraża politykę i strategię ochrony cyberprzestrzeni.

Analiza istoty ochrony cyberbezpieczeństwa, której podmiotem jest Unia Europejska, pozwoli na wykazanie, że istnieje polityka cyberbezpieczeństwa w UE, która jest oparta na bezpieczeństwie informacyjnym i podlega ewolucji. Tym samym mamy do czynienia z procesem niezakończonym. W celu analizy przedmiotu ochrony cyberbezpieczeństwa UE, czyli działań związanych ze zwalczaniem zagrożenia cyberterroryzmem, należy wykonać badanie wstępne polegające na zdefiniowaniu istoty i zakresu cyberterroryzmu oraz uwarunkowań zagrożeń cyberterrorystycznych w Unii. Określenie przyczyny powstania zjawiska cyberterroryzmu we Wspólnocie Europejskiej (czynniki wewnętrzne i zewnętrzne) pozwoli na stwierdzenie, jaki wpływ zjawisko cyberterroryzmu wywiera na politykę UE, oraz wykaże, że przyczyną zainteresowania się polityką cyberbezpieczeństwa jest także brak odpowiednich mechanizmów i regulacji w tym zakresie, w związku z czym mamy do czynienia z procesem zarówno instytucjonalizacji, jak i transformacji.

Nie można tego uczynić bez wyjaśnienia, czym jest paradygmat bezpieczeństwa państwa oraz jak on ewoluuje. Analiza paradygmatu bezpieczeństwa zawierającego podmiot bezpieczeństwa, przedmiot bezpieczeństwa, środowisko, w którym bezpieczeństwo to jest zapewniane lub realizowane, oraz interakcje między wymienionymi składowymi, pozwoli na stwierdzenie, że dzieje się to w związku z umiejętnością jego zagwarantowania w stosunku do wartości, potrzeb, interesów, celów, które warunkują realizację polityki i strategii państwa w perspektywie krótko-, średnio- i długoterminowej[6]. Będzie to miało na celu wykazanie, w jaki sposób polityka i strategia oddziaływają na siebie, ze szczególnym uwzględnieniem koncepcji bezpieczeństwa UE. Rozważania na temat *Europejskiej strategii bezpieczeństwa* (ESB) przedstawią i zwrócą

uwagę na znaczenie strategii bezpieczeństwa jako instrumentu polityki cyberbezpieczeństwa Unii. Z kolei analiza strategii cyberbezpieczeństwa, czyli metody realizacji polityki bezpieczeństwa systemu informacyjnego będącej adaptacją metod stosowanych w szeroko pojętej problematyce bezpieczeństwa życia społecznego, przedstawi istotę jej koncepcji oraz zmiany, jakie nastąpiły przez lata, aby na koniec ukazać i przeanalizować, na czym polega zakres obecnej strategii ochrony UE w cyberprzestrzeni.

Analiza podstaw normatywnych pozwoli na wykazanie zależności polityki ochrony cyberprzestrzeni od poziomu integracji państw członkowskich. Wykaże związek funkcjonalny zachodzący między harmonizacją przepisów prawa państwowego (na wybranych przykładach) a prawem unijnym w dziedzinie ochrony cyberbezpieczeństwa, chociaż proces ten postępuje powoli. Analiza realizacji polityki ochrony cyberprzestrzeni umożliwi natomiast poznanie instrumentów, za pomocą których Unia realizuje funkcje ochronne na poziomach państwowym i unijnym, oraz zależności problemów bezpieczeństwa wewnętrznego UE, a tym samym polityki ochrony cyberprzestrzeni, od poziomu integracji państw członkowskich.

Dzięki wnikliwej analizie implementacji polityki i strategii ochrony cyberbezpieczeństwa na przykładzie wybranych państw Unii zostaną wskazane różnice zachodzące na poziomie państwowym dotyczące strategii, procedury realizacji polityki cyberbezpieczeństwa, instytucji i podstaw prawnych, co przekłada się na skuteczność zwalczania tego zjawiska. Analiza podstaw normatywnych pozwoli na wykazanie zależności ochrony cyberprzestrzeni od poziomu integracji państw członkowskich, w szczególności od nowych zagrożeń i wyzwań dla cyberbezpieczeństwa. Z kolei międzykulturowa analiza porównawcza, obejmująca systemy prawne wraz ze strategiami różnych państw pod kątem dostosowania ich do aktualnych wymagań cywilizacyjnych związanych z przyspieszającą cyfryzacją oraz pod kątem zdolności wykorzystania szans i potencjałów wynikających z gwałtownych i głębokich zmian cywilizacyjnych ze szczególnym uwzględnieniem zagadnień cyberbezpieczeństwa,

wykaże nie tylko istnienie związku funkcjonalnego zachodzącego między harmonizacją przepisów prawa państwowego (Polski, Niemiec, Wielkiej Brytanii, Francji i Estonii) a prawem unijnym w dziedzinie bezpieczeństwa, lecz także że polityka cyberbezpieczeństwa jest zjawiskiem wielopłaszczyznowym, na które składa się zestaw procesów i czynników tworzących również ramy cyberstrategii każdego państwa.

Należy podkreślić, że współcześnie właściwa i skuteczna ochrona dostępu do systemów informatycznych jest czynnikiem decydującym o bezpieczeństwie informacji. Odpowiedzialność za dany wybór i ustanowienie środków zabezpieczających spoczywa na właścicielach systemów, ich zarządcach i administratorach. Jak podkreśla Andrzej Adamski[7], środkom karnym przypada w tym zakresie rola zdecydowanie pomocnicza.

Ramy czasowe pracy obejmują ochronę cyberbezpieczeństwa UE od momentu przyjęcia Traktatu o Unii Europejskiej do chwili brexitu, ponieważ wyjście Wielkiej Brytanii może w znacznym stopniu osłabić cyberobronę całej Wspólnoty. Wydaje się to możliwe mimo wprowadzenia w życie nowych norm, np. dyrektywy NIS, gdyż obecnie to właśnie Wielka Brytania jest uważana za supermocarstwo w cyberprzestrzeni[8]. Wszelkie działania podjęte w tej materii przed uchwaleniem Traktatu o Unii Europejskiej (TUE) traktowane są jako geneza polityki będącej przedmiotem badania.

Na podstawie przeprowadzonej analizy zagadnienia weryfikacji poddano cztery tezy badawcze. Po pierwsze, należy przyjąć, że polityka ochrony cyberprzestrzeni ewoluuje i zmierza do harmonizacji norm prawnych przyjętych w prawie UE, chociaż proces ten postępuje z różną prędkością w każdym państwie członkowskim i nie należy go uznawać za zakończony.

Po drugie, przyczyną powstania tej polityki i jej ewolucja jest reakcją na wzrost niestabilności i zagrożeń w tym obszarze oraz brak odpowiednich mechanizmów i regulacji w tym zakresie, w związku z czym mamy do czynienia zarówno z procesem instytucjonalizacji, jak i transformacji. Określenie przyczyny powstania zjawiska cyberterroryzmu w Unii Europejskiej (czynniki wewnętrzne i

zewnętrzne) pozwoli na stwierdzenie, jak zjawisko cyberterroryzmu wpływa na politykę i strategię ochrony cyberprzestrzeni UE.

Po trzecie, w obliczu dynamiki zmian w środowisku międzynarodowym dotychczasowe postrzeganie bezpieczeństwa informacyjnego wymaga jego redefinicji i wzmocnienia współpracy nie tylko między państwami członkowskimi UE, lecz także z państwami trzecimi. Nie ulega jednak wątpliwości, że prawo cyberprzestrzeni będzie się przez wiele lat stopniowo kształtować. Technologia, a w szczególności technologia informatyczna, rozwija się w szybkim tempie. Prawa międzynarodowe, regionalne i krajowe pozostają o krok za innowacjami technologicznymi. Postępu nie można zatrzymać, należy więc skierować go na właściwe tory prawne – stworzyć nowe lub przekształcić stare normy postępowania, aby były odpowiednie w przestrzeni o transgranicznym i transnarodowym charakterze. Rozwiązania przyjęte w prawie cyberprzestrzeni powinny wyróżniać się kilkoma cechami. Powinny być przede wszystkim neutralne technologicznie, aby prawo odpowiadało postępowi w technice i innowacyjnym rozwiązaniom. Nie mogą doprowadzać do zjawiska „nadregulacji", dlatego zostanie podjęta próba wykazania, że prawo unijne jest właściwym instrumentem służącym harmonizacji i uwspólnotowieniu regulacji prawa krajowego w cyberprzestrzeni pod warunkiem tworzenia reguł współpracy między Unią a państwami członkowskimi, w myśl art. 72–73 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE).

Po czwarte, im większy poziom wzmacniania współpracy między państwami i mechanizmów implementacji wewnątrzunijnych w obliczu zjawiska cyberprzestepczości, tym większe prawdopodobieństwo stabilności i bezpieczeństwa w Unii Europejskiej i krajach członkowskich. Ponieważ zjawisko cyberterroryzmu ma charakter transgraniczny, ochrona cyberprzestrzeni powinna opierać się na współpracy międzypaństwowej i koordynacji działań, które stanowią nieodzowny element skutecznej odpowiedzi na cyberterroryzm. W związku z tym nasuwają się zasadnicze pytania, w jakim kierunku powinna zmierzać współczesna polityka i strategia zwalczania cyberterroryzmu na gruncie instytucjonalno-prawnym Unii oraz w

jakim zakresie umiejętnie prowadzona strategia i polityka ochrony cyberbezpieczeństwa jest w stanie wywrzeć wpływ na bezpieczeństwo wewnętrzne poszczególnych państw członkowskich.

Na strukturę monografii składa się siedem rozdziałów. W pierwszym – *Geneza i istota bezpieczeństwa informacyjnego Unii Europejskiej* – wyjaśniono istotę zjawiska cyberterroryzmu i cyberprzestępczości oraz ich wpływ na politykę bezpieczeństwa państwa w społeczeństwie informacyjnym. Przedmiotem analizy jest geneza oraz rozwój polityki cyberbezpieczeństwa UE, która podlega ewolucji, a proces ten nie został zakończony. Rozdział ten stanowi wprowadzenie do badanego problemu. W jego pierwszej części zaprezentowano działania Unii Europejskiej podjęte przed Traktatem o Unii Europejskiej. Celem wyznaczenia ram dla dalszych rozważań określono zakres polityki Unii. W drugiej części przedstawiono istotę i specyfikę polityki cyberbezpieczeństwa wynikającą z usytuowania w strukturze UE.

Drugi rozdział – *Strategia cyberbezpieczeństwa Unii Europejskiej w XXI wieku* – poddaje analizie paradygmat bezpieczeństwa i stara się wyjaśnić, jak paradygmat bezpieczeństwa oraz koncepcje bezpieczeństwa ewoluowały po II wojnie światowej, a także w jaki sposób wpłynęło to na politykę i strategie państw, ze szczególnym uwzględnieniem koncepcji bezpieczeństwa UE. W pierwszej części wyjaśnia pojęcie paradygmatu, różnice między poszczególnymi paradygmatami bezpieczeństwa, aby ostatecznie przedstawić jego miejsce w naukach o bezpieczeństwie. Druga część rozdziału została poświęcona rozważaniom na temat *Europejskiej strategii bezpieczeństwa* i znaczeniu strategii bezpieczeństwa jako instrumentu polityki cyberbezpieczeństwa UE. Z kolei analiza ESB ukazuje zmiany w istocie koncepcji jej pojmowania, jakie nastąpiły przez lata. Na koniec przedstawiono i przeanalizowano zakres obecnej strategii ochrony UE w cyberprzestrzeni.

W trzecim rozdziale – *Uwarunkowania polityki cyberbezpieczeństwa Unii Europejskiej* – przedmiotem analizy jest istota i specyfika cyberterroryzmu jako formy przemocy. W pierwszej jego części przeanalizowano cyberterroryzm jako zagrożenie w XXI w. z odwołaniem się do konkretnych przykładów. W drugiej części

przedstawiono i poddano analizie czynniki warunkujące zagrożenie cyberterrorystyczne UE oraz przyczyny tworzące to zagrożenie. Określenie czynników wewnętrznych i zewnętrznych przyczyniających się do występowania cyberterroryzmu w Unii pozwoli wskazać jego wpływ na politykę bezpieczeństwa UE, a także udowodnić, że podstawą wprowadzenia polityki ochrony cyberprzestrzeni był brak odpowiednich mechanizmów i regulacji w tym zakresie. W związku z tym mamy do czynienia z procesem zarówno instytucjonalizacji, jak i transformacji, a konsekwencją jest przedmiotowe ujęcie tego zagadnienia i omówienie podziału uwarunkowań z uwzględnieniem zagrożeń globalnych i lokalnych.

W pierwszym podrozdziale (*Prawne standardy cyberbezpieczeństwa Unii Europejskiej*) poddano analizie międzynarodowe standardy zwalczania cyberterroryzmu zawarte w różnych konwencjach międzynarodowych. W następnych podrozdziałach przedstawiono zagadnienia prawne polityki ochrony cyberprzestrzeni UE z podziałem na prawo pierwotne i wtórne ze względu na to, że prawo ochrony cyberprzestrzeni UE należy traktować jako szczególny przypadek prawa międzynarodowego. Ukazano wpływ prawa międzynarodowego obowiązującego przed powstaniem Unii Europejskiej na obecny kształt prawa unijnego. Przeprowadzono również analizę procesu uwspólnotowienia polityki cyberbezpieczeństwa UE na podstawie przyjętych rozwiązań prawnych. Analiza podstaw prawnych pozwoliła na wykazanie zależności polityki cyberbezpieczeństwa od poziomu integracji państw członkowskich, a także związku funkcjonalnego zachodzącego między harmonizacją przepisów prawa państwowego a prawem unijnym w dziedzinie bezpieczeństwa, ponieważ proces ten trwa.

Przedmiotem analizy piątego rozdziału – *Realizacja polityki cyberbezpieczeństwa Unii Europejskiej* – jest wprowadzanie w życie polityki ochrony cyberprzestrzeni UE, w której podmiotem jest Unia Europejska. Ponieważ zmiany w polityce cyberbezpieczeństwa są reakcją na wzrost niestabilności i zagrożeń oraz brak odpowiednich mechanizmów i regulacji w tym zakresie, analiza realizacji polityki cyberbezpieczeństwa umożliwi poznanie instrumentów, za pomocą

których Unia urzeczywistnia funkcje ochronne na poziomie państwowym i poziomie europejskim, oraz wskazanie zależności problemów bezpieczeństwa wewnętrznego UE, a tym samym polityki ochrony cyberprzestrzeni, od poziomu integracji państw członkowskich. W tym rozdziale określono podmiot i przedmiot polityki cyberbezpieczeństwa, przedstawiono i oceniono też instrumenty stosowane przez Unię w prowadzonej przez nią polityce ochrony cyberprzestrzeni. Przyjęto tutaj podział na działania odnoszące się do wnętrza UE oraz skierowane na zewnątrz. Do pierwszych należą instrumenty dotyczące walki z cyberprzestępczości i ochrony cyberprzestrzeni, te drugie natomiast dotyczą ochrony praw własności intelektualnej i handlu w Internecie i opierają się na współpracy z państwami. Drugi rodzaj instrumentów nie stanowił przedmiotu pogłębionych badań.

Szósty rozdział – *Implementacja polityki cyberbezpieczeństwa w Unii Europejskiej na przykładzie wybranych państw* – poświęcono implementacji polityki i strategii cyberbezpieczeństwa w wybranych państwach członkowskich UE. Analiza implementacji polityki ochrony cyberprzestrzeni na przykładzie Polski, Niemiec, Wielkiej Brytanii, Francji i Estonii stanowiła przedmiot badawczy tego rozdziału i umożliwiła poznanie instrumentów, za pomocą których Unia realizuje funkcje ochronne na poziomie wewnątrzpaństwowym i europejskim, oraz zależność problemów bezpieczeństwa wewnętrznego UE, a tym samym polityki cyberbezpieczeństwa od poziomu integracji państw członkowskich. Wybór państw został podyktowany ich pozycją w Europie i na świecie oraz sposobem prowadzenia strategii w cyberprzestrzeni. Analizie poddano zarówno liderów, jak i ofiary ataków cyberterrorystycznych. Zwrócono uwagę przede wszystkim na aspekt zgodności polityki wewnętrznej danego państwa członkowskiego w tej kwestii z polityką ochrony cyberprzestrzeni UE. Uwzględniono takie zagadnienia, jak dostosowanie przepisów prawa wewnętrznego do prawodawstwa unijnego przy jednoczesnym przestrzeganiu prawa. Pozwoliło to na wskazanie, które z analizowanych państw członkowskich prowadzi politykę antyterrorystyczną najbardziej zgodną z polityką UE.

Siódmy rozdział – *Skutki i perspektywy rozwoju strategii i polityki cyberbezpieczeństwa Unii Europejskiej* – składa się z dwóch części. W pierwszej przedstawiono skutki strategii i polityki cyberbezpieczeństwa UE. Ujęto je w kategoriach zmian zarówno dla Unii, jak i dla państw członkowskich. W drugiej części przedstawiono trzy scenariusze perspektywy rozwoju strategii i polityki Unii. Rozpatrując scenariusze dla przyjętych modeli systemu społecznego i hipotez dotyczących zmian społecznych, można – stosując metodę analizy prognostycznej GSO – przyjąć scenariusz pesymistyczny sprzyjający „grze indywidualnych interesów", w którym podstawowymi zasobami są informacja i wiedza. Zagrożeniem jest natomiast atomizacja zachowań społecznych wraz z „atrofią więzi" międzyludzkich. Drugi jest scenariuszem pośrednim sprzyjającym „grze grup interesów", której „wygraną" jest dostęp do wiedzy jako podstawowego zasobu, a zagrożeniem swoisty „cyberautokratyzm". Trzeci scenariusz jest optymistyczny, sprzyjający dostępowi do wiedzy i mądrości w interesie całego społeczeństwa oraz rozwojowi społeczeństwa cyfrowego.

Taki układ publikacji pozwala na przejrzyste i jasne przedstawienie problematyki, a to z kolei daje możliwość wyprowadzenia wniosków oraz przedstawienia wizji rozwoju polityki antyterrorystycznej Unii na podstawie przeprowadzonych badań i obserwacji. Temat i charakter pracy uniemożliwiają jednak całkowite rozdzielenie wszystkich wątków, w związku z czym w pewnych miejscach nakładają się one na siebie.

Podstawę źródłową przeprowadzonej analizy stanowią dokumenty Unii Europejskiej, Polski, Niemiec, Francji, Estonii i Wielkiej Brytanii, regulujące problematykę cyberterroryzmu. Do przeprowadzonych analiz wykorzystano akty prawne (przede wszystkim traktaty, dyrektywy i rozporządzenia) oraz materiały znajdujące się na stronach: ONZ, Rady Europy, Unii Europejskiej, parlamentów wybranych państw członkowskich (strategie narodowe i ustawy), orzeczenia Europejskiego Trybunału Sprawiedliwości (ETS) i sądów krajowych oraz materiały zamieszczone na stronie internetowej Instytutu Strategicznego. Na ten temat powstało również wiele raportów międzynarodowych przygotowanych przez

organy UE czy NATO (Europol 2014–2019, ENISA 2015–2020, NATO StratCom) oraz oficjalnych stron międzynarodowych organów ścigania (Interpol). Dostęp do materiałów źródłowych (przeważnie angielsko-, niemiecko- i francuskojęzycznych) był możliwy dzięki Internetowi, głównie dostępowi do bazy danych serwisu europa.eu. Ze względu na szybko ewoluującą politykę UE wobec procesu cyberterroryzmu istotne były liczne, opublikowane w Internecie, materiały statystyczne, pokonferencyjne, prasowe i artykuły naukowe związane z tym zagadnieniem.

Pozyskanie tak wielu materiałów było możliwe dzięki wieloletniemu procesowi gromadzenia literatury, licznych pozycji naukowych, przede wszystkim literatury obcojęzycznej. Należą do nich m.in. publikacje: T.R. Aleksandrowicz, K. Liedel, *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia*, w: K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, Warszawa 2014; A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003; H. Carrapico, A. Barrinh, *The EU as coherent (cyber) security actor?*, „Journal of Common Market Studies" 2017, vol. 55 (6); P. Dela, *Zasady sztuki wojennej w cyberprzestrzeni*, w: A. Polak, J. Lasota, M. Palczewska (red.), *Wojny i konflikty zbrojne XXI wieku – podejście polemologiczne*, Warszawa 2016; J. Gryz (red.), *Zarys teorii bezpieczeństwa państwa*, Warszawa 2016; R. Kuźniar, *Europejska strategia bezpieczeństwa,* „Polska w Europie" 2004, nr 2 (46); K. Kjærgaard-Christensen, T. Liebetrau, *A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry*, „Intelligence and National Security" 2019, vol. 34 (3); M. Madej, *Instytucjonalizacja współpracy międzynarodowej w dziedzinie zwalczania terroryzmu w Europie*, w: S. Parzymies, R. Zięba (red.), *Instytucjonalizacja wielostronnej współpracy międzynarodowej w Europie*, Warszawa 2004; S. Malešević, *Terrorism. In The Rise of Organised Brutality: A Historical Sociology of Violence*, Cambridge 2017; C. McLeish, *Recasting the Threat of Chemical Terrorism in the EU: The Issue of Returnees from the Syrian Conflict*, „European Journal of Risk Regulation" 2017, nr 8(4); P. Mickiewicz, *System*

bezpieczeństwa narodowego w rozwiązaniach systemowych wybranych państw, Warszawa 2018; E. Milczarek, *Współczesne wyzwania ochrony bezpieczeństwa informacyjnego jednostki w Internecie*, w: M. Porzeżyński, A. Borcuch (red.), *Bezpieczeństwo w erze społeczeństwa informacyjnego. Wyzwania w sferach kultury, marketingu i gospodarki*, Kielce 2019; A. Moravcsik, *Taking Preferences Seriously: A Liberal Theory of International Politics*, „International Organization" 2007, nr 4(51); K. Oppermann, *The Politics of Avoiding Referendums on the Treaty of Lisbon,* „Journal of European Integration" 2013, vol. 35(1); M. Pietraś, *Bezpieczeństwo międzynarodowe*, w: M. Pietraś (red.), *Międzynarodowe stosunki polityczne*, Lublin 2007; V. Pitts, *Cyber Crimes: History of World's Worst Cyber Attacks*, Marousi 2017; W. Pokruszyński, *Polityka – Teoria – Bezpieczeństwo*, Józefów 2012; S. Wojciechowski, *Reasons of Contemporary Terrorism. An Analysis of Main Determinants*, w: A. Sroka, F. Castro-Rial Garrone, R. Torres Kumbrian (red.), *Radicalism and Terrorism in the 21st Century*, Frankfurt am Main–Bern–Bruxelles–New York–Oxford–Warszawa–Wien 2017; P. Zherestov, *From visible pasts to an invisible presence: new criminological reality after planetary cyber attack 12/05/17 Wannacry*, „Przegląd Wschodnioeuropejski" 2018, nr 2.

Praca ma charakter interdyscyplinarny, obejmuje zagadnienia z zakresu nauk o bezpieczeństwie, stosunków międzynarodowych, prawa międzynarodowego i unijnego, co stało się podstawą szerokiej i wnikliwej analizy materiałów i tekstów źródłowych. Przy przedstawianiu zjawiska terroryzmu w Unii Europejskiej wykorzystano kilka metod badawczych, ponieważ złożoność polityki ochrony cyberbezpieczeństwa uniemożliwia zastosowanie jednej z nich. Punkt wyjścia badań stanowiły kwerendy źródłowe i studia literaturowe mające na celu wspólne określenie profilów kompetencyjnych kluczowych z punktu widzenia wyzwań cyberbezpieczeństwa. Następnie poddano analizie i ocenie najważniejsze prawne i polityczno-strategiczne dokumenty programowe UE i wybranych państw pod kątem zawartych w nich wizji społeczeństwa informacyjnego, ze szczególnym uwzględnieniem wyzwań dla cyberbezpieczeństwa.

W badaniu odwołano się do metody ilościowej w celu stwierdzenia, jak wraz z rozwojem w czasie cyfryzacji i technologii kształtowała się polityka ochrony cyberprzestrzeni UE. Za pomocą analizy czynnikowej ustalono wpływ poszczególnych czynników na zjawisko cyberterroryzmu. Następnie zastosowano metodę decyzyjną, aby poznać wpływ, jaki wywierają poszczególne instrumenty stosowane przez Unię w ramach polityki ochrony cyberprzestrzeni na zjawisko cyberterroryzmu. Wykorzystano także metodę prawnoporównawczą w celu ustalenia zgodności polityki wewnętrznej wybranych państw członkowskich z polityką ochrony cyberprzestrzeni UE. Z kolei technika analizy dokumentów pozwoliła na zbadanie zawartości aktów prawnych regulujących problematykę cyberterroryzmu w Unii. Metoda analizy orzecznictwa pozwoliła na porównanie i określenie, w jaki sposób kształtuje się praktyka sądowa w wybranych państwach. Technika statystyczna natomiast umożliwiła uporządkowanie spostrzeżeń naukowych. Zastosowano również technikę prognostyczną w celu przedstawienia wizji rozwoju polityki ochrony cyberprzestrzeni UE. Jako końcową wybrano metodę syntezy całości zjawiska na podstawie dotychczas przeprowadzonych obserwacji.

1

GENEZA I ISTOTA BEZPIECZEŃSTWA INFORMACYJNEGO

Obecnie każdy obszar działalności człowieka i państwa coraz częściej staje się zależny od dostarczenia informacji i funkcjonowania systemów opartych na informacjach. Wojsko, gospodarka, energetyka, media, systemy bankowe i komunikacyjne są w dużym stopniu oparte na systemach informacyjnych, które odgrywają decydującą rolę w procesie podejmowania decyzji w organizacjach cywilnych i wojskowych. Oznacza to, że większego znaczenia nabiera „pozytywne" ujęcie bezpieczeństwa informacyjnego w odróżnieniu od tradycyjnego („negatywnego" ujęcia jako stanu wolnego od zagrożeń), kładąc akcent na „tworzenie optymalnych warunków wewnętrznego bezkonfliktowego rozwoju istotnych składników danego systemu oraz eliminowanie jego ewentualnego zewnętrznego zagrożenia przez przyczynianie się do takiego ukształtowania otoczenia zewnętrznego, które by sprzyjało harmonijnemu, symbiotycznemu rozwojowi"[9].

Rozdział ten stanowi wprowadzenie do całości monografii. Przedmiotem analizy jest geneza bezpieczeństwa informacyjnego oraz rozwój polityki cyberbezpieczeństwa Unii Europejskiej (UE). Analiza genezy bezpieczeństwa informacyjnego i polityki cyberbezpieczeństwa UE pozwoliła na wykazanie, że istnieje polityka cyberbezpieczeństwa UE, która jest oparta na bezpieczeństwie

informacyjnym i podlega ewolucji, oraz że mamy do czynienia z procesem, który nie został zakończony. Rozdział ten stanowi wprowadzenie do badanego problemu.

W pierwszej części pokazano działania Unii Europejskiej podjęte przed Traktatem o Unii Europejskiej, a co za tym idzie genezę bezpieczeństwa informacyjnego Unii, rozpoczynając w ten sposób rozważania dotyczące polityki i strategii cyberbezpieczeństwa Wspólnoty. Ponieważ przedmiotem analizy jest bezpieczeństwo informacyjne podejmowane w ramach polityki i strategii cyberbezpieczeństwa w wymiarze instytucjonalno-prawnym, zarówno na poziomie Unii, jak i na poziomie państwowym, związane ze zwalczaniem zagrożenia cyberterroryzmem oraz analiza podejmowanych w tym kierunku działań, dlatego w celu wyznaczenia ram dalszych rozważań przedstawiono definicję pojęć z zakresu bezpieczeństwa informacyjnego.

W drugiej części zaprezentowano istotę i specyfikę polityki bezpieczeństwa informacyjnego UE względem polityki ochrony cyberprzestrzeni wynikającą z usytuowania jej w strukturze Unii.

1.1
GENEZA BEZPIECZEŃSTWA INFORMACYJNEGO W UNII EUROPEJSKIEJ

Współczesne pojmowanie bezpieczeństwa zakłada jego kompleksowe traktowanie. Obecnie zwraca się uwagę na militarne i pozamilitarne aspekty tej problematyki oraz jej personalne i strukturalne konteksty. Bezpieczeństwo jest potrzebą podmiotową, co oznacza, że może dotyczyć danego rodzaju podmiotów – od jednostek po wielkie grupy społeczne, włączając w to struktury organizacyjne (instytucje) reprezentujące pojedynczych ludzi oraz grupy społeczne (państwa, narody, system międzynarodowy). Bezpieczeństwo jest pierwszoplanowym zadaniem państwa[10]. Jego zapewnienie jest konieczne do stworzenia określonych warunków do

działalności i rozwoju społeczeństwa. Podstawowe interesy narodowe są niezmienne i oparte na całościowej koncepcji bezpieczeństwa uwzględniającej aspekty polityczne, ekonomiczne, społeczne i militarne[11]. Ich realizacja z kolei stanowi dla państwa i jego mieszkańców potrzebę nadrzędną. Bezpieczeństwo jest z jednej strony określoną wartością społeczną, cywilizacyjną, kulturową, polityczną, ekonomiczną i ekologiczną, z drugiej zaś – wartością egzystencjalną, moralną i duchową. Jest również wartością fundamentalną, do której nie dąży się ze względu na nią samą, ale ze względu na inne wartości, które ona zabezpiecza[12].

Poprawne funkcjonowanie społeczeństwa jest uzależnione w dużym stopniu od funkcjonowania nowoczesnych technik i technologii informacyjnych. Komputery i sieci komputerowe są powszechnie wykorzystywane w gospodarce, administracji i gospodarstwach domowych. Urządzenia te stają się niezbędne do sterowania wszystkimi nowoczesnymi procesami zarządzania, administrowania, kontroli, a także dostarczania towarów i usług. Poza niekwestionowanymi korzyściami niosą również liczne zagrożenia. Jednym z nich jest jakościowa przemiana przestępczości. Tradycyjne formy i sposoby popełniania przestępstw są zastępowane przez metody wykorzystujące wszelkie możliwości nowoczesnych technologii[13].

Wieki temu niektórzy myśliciele rozpatrywali zjawisko wirtualnej rzeczywistości, które nosiło wiele cech obecnego pojmowania cyberprzestrzeni. Filozof starożytnej Grecji Platon w swoim dziele *Państwo* pisał o świecie postrzeganym przez ludzi jako cień świata rzeczywistego i materialnego, w którym ludzie żyją zanurzeni w jakiejś wirtualnej przestrzeni, uznając ją niesłusznie za realną. Interesującym ujęciem jest koncepcja noosfery (od gr. *noos* – duch), czyli wizji ewoluującego świata, którą opracował w pierwszej połowie XX w. jezuita Pierre Teilhard de Chardin. Jej istotą jest teoria neoogenezy, czyli procesu rozwoju świadomości wszystkich: przeszłych, teraźniejszych i przyszłych ludzi na Ziemi. To kulturowo-cywilizacyjny dorobek człowieka unoszący się nad geosferą i biosferą jako jeszcze jedna warstwa oplatającą naszą planetę. Noosfera

wydaje się ważną ideą pozwalającą zrozumieć istotę Internetu. Choć jednostki pokoleń w noosferze rodzą się wciąż tak samo ograniczone biologicznie, to zastają coraz bogatszą w skali okołoziemskiej macierz kulturowo-cywilizacyjną. Jest to dla nich nieograniczona szansa bycia czymś więcej, to znaczy przyrostu świadomości, wolności i personalizacji. W teoretycznym założeniu noosfera nie jest anonimową ogólnoludzką termitierą, lecz jednością, w której niepowtarzalna osoba ludzka doznaje spełnienia[14].

Konstrukcja współczesnego modelu społeczeństwa informacyjnego, którego niezaprzeczalnym katalizatorem są technologie stosowane podczas komunikacji elektronicznej przybierającej w wyniku konwergencji formę cyfrową, wyzwala potrzebę refleksji nad fenomenem informacji. Jednym z pierwszych autorów zajmujących się rzeczywistością wirtualną i pomysłodawcą terminu *cyberspace* jest William Gibson. Zaobserwował on, że cyberprzestrzeń kreuje nowe, niejako równoległe środowiska stworzone przez komputery i nadaje całkiem inny wymiar ludzkiemu funkcjonowaniu. Cyberprzestrzeń według niego to „odruchowa halucynacja, której codziennie doświadczają miliardy ludzi, w każdym narodzie, dzieci nauczane matematycznych koncepcji [...] graficzne odzwierciedlenie w ludzkim umyśle danych z zasobów każdego komputera. Niewyobrażalna złożoność. Linie świetlne wycelowane w antyprzestrzeń ludzkiego umysłu. Klastry i konstelacje danych. Jak niezliczone światła wielkiego miasta”[15].

Pierre Lévy określa cyberprzestrzeń jako „przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących w całym świecie”[16]. Z kolei Marian Golka uważa, że cyberprzestrzeń to „przestrzeń komunikowania się przez Internet oraz wszelkie nośniki danych cyfrowych. Jest to oczywiście przestrzeń nieokreślona, bez możliwości wyobrażenia jej sobie w wymiarze fizycznym”[17].

W związku z tym przestrzeń internetowa oznacza:

- ograniczenie doświadczeń doznawanych za pomocą zmysłów,
- płynność tożsamości oraz anonimowość,
- zrównanie stosunków społecznych użytkowników,

- pokonywanie ograniczeń przestrzennych,
- rozciąganie i koncentracja czasu,
- dostępność wielu kontaktów,
- nieoczekiwane wyłączenie się z kontaktu jego niektórych uczestników,
- możliwość permanentnego zapisu,
- odmienne stany świadomości[18].

Kluczową częścią cyberprzestrzeni jest rzeczywistość wirtualna, którą Manuel Castells definiuje jako „system, w którym sama rzeczywistość (tzn. materialna/symboliczna egzystencja ludzi) jest całkowicie schwytana, w pełni zanurzona w wirtualnym układzie obrazów, w świecie wyobraź-sobie-że, w którym pozory nie tylko znajdują się na ekranie, za pośrednictwem którego komunikuje się doświadczenie, lecz stają się tym doświadczeniem” [19]. Istota rzeczywistości wirtualnej pozostaje nadal nieokreślona.

Wolfgang Welsch[20] zauważył, że skoro zbiory danych cyfrowych mogą w jednej chwili rozrastać się, przekształcać, rozrywać, łączyć ze sobą i krzyżować, to mamy do czynienia z brakiem wyraźnej i przekonywającej różnicy między bytem a zjawiskiem, które sygnalizuje ten byt, między istotą rzeczy a jej obrazem, między rzeczywistością a złudzeniem. W efekcie zamiast stabilności mamy zmienność, zamiast głębi – powierzchowność, zamiast rzeczywistości – iluzję i możliwość[21]. Częsta obecność rzeczywistości wirtualnej w komunikowaniu sprawia, że użytkowników nie interesuje prawda, przestaje też być kryterium oceny świata i zdarzeń w nim zachodzących. Zdaniem Stanisława Lema rzeczywistość wirtualna jest w rozumieniu odbiorców traktowana jako wirtualna, ale może przyjść taki czas, kiedy zaczniemy mieć autentyczne trudności z jej odróżnieniem od rzeczywistości realnej[22].

Należy przypomnieć, że pojęcie „wirtualny” pochodzi z języka łacińskiego od słowa *virtus* oznaczającego męstwo, energię. Władysław Kopaliński w *Słowniku wyrazów obcych* określa słowo „wirtualny” jako „teoretycznie możliwy, mogący zaistnieć”[23]. W

języku niemieckim oznacza m.in. „potencjalność, możliwość zaistnienia, pozorność", a w języku angielskim – „faktyczność" czy „prawdziwość".

Wirtualność można więc określać jako:

- symultaniczność – nie jest ona „realną realnością", wirtualność czerpie z realności, a realność czerpie z wirtualności, wskutek doświadczania wirtualności obserwujemy rozszerzenie możliwości naszych doznań wizualnych;
- doznanie u widza impresji, czyli „zanurzenia zmysłowego" – jej efektem jest nieodróżnianie bodźców wirtualnych od realnych, a przy tym pełna iluzja bycia w innym świecie przy poczuciu odcięcia od realnego świata zewnętrznego;
- interaktywność – kontakty użytkownika ze światem dostępnym dzięki komputerowi, poczucie dematerializacji komputera, traktowanie własnego ciała jako rodzaju łącznika;
- teleobecność – obecność w nieokreślonej przestrzeni Internetu, na licznych serwerach różnorodnych treści zapisanych cyfrowo z możliwością ich aktualizacji, przekształcenia i przesłania dalej[24].

Wirtualność przejawia się w różnych sprawach realnych. Przykładem mogą być pieniądze w zapisie cyfrowym za pomocą digitalnych znaków określających ich wartość, ich właściciela i ich położenie czy podpis elektroniczny zastępujący tradycyjny, będący sekwencją cyfr i pozostający jedynie teoretyczną umownością. Przejawem wirtualności są też społeczności internetowe mające związek z różnymi przejawami wirtualnych rzeczywistości. Rzeczywistość wirtualna jako forma działalności społeczeństwa i komunikowania między ludźmi to niespotykane wcześniej zjawisko o takim charakterze, na niespotykaną wcześniej skalę.

Powstanie i rozwój cyberprzestrzeni jest nierozerwalnie związany z rozprzestrzenianiem się sieci Internet, która najczęściej określana jest jako globalna sieć komputerowa, czyli sieć sieci. Cyberprzestrzeń jest równoległą przestrzenią niefizyczną, niekonkurencyjną w stosunku do przestrzeni trójwymiarowej. Budulcem cyberprzestrzeni są dane i informacje, które przez wzajemne oddziaływania między

sobą kreują mikrokorelacje. Między przestrzenią trójwymiarową a cyberprzestrzenią zachodzą natomiast makrokorelacje. Ich charakter jest interpersonalny. Makrokorelacje są każdą postacią komunikacji zachodzącej między jednostkami. Polegają na wprowadzaniu do cyberprzestrzeni informacji w różnej postaci formatu utrwalenia, ich odbiorze połączonym z określoną projekcją w ludzkiej umysłowości oraz wielokrotnym ich wykorzystaniem. Proces makrokorelacji ma charakter ciągły, niezależny od przestrzeni i w znacznie mniejszym zakresie niż dotychczasowe metody relacji interpersonalnych zależy od czasu. Konsekwencją jego powstania jest społeczeństwo informacyjne. Jest on sprzęgnięty z przemianami technologicznymi, mając niewątpliwie humanistyczne i przyrodnicze (antropologiczne) konsekwencje[25].

Można postawić tezę, że nowe zjawiska technologiczne w dziedzinie przesyłania danych i informacji modelują obszary wzajemnych ludzkich oddziaływań[26]. Na tym gruncie zasadzają się zwyczaje i potrzeby regulacji prawnych. Komunikacja elektroniczna doprowadziła do powstania zbiorowości, w której koegzystencja przybrała nową jakość[27].

Ludzkie stosunki kwalifikowane jurydycznie są w przestrzeni nowych zjawisk poddane innemu wartościowaniu. Takie ujęcie ludzkiej zbiorowości wywodzi się z uświadomienia intensywności społecznych oddziaływań i nowej płaszczyzny dla ich urzeczywistniania – cyberprzestrzeni. Zasięg nowej formy koegzystencji jednostek, kwalifikowanej wybiórczo i niespójnie przez normy prawne, jest wręcz globalny. Jego układ jest równoległy i „niekonkurencyjny” w stosunku do desygnatów innych form opisu ludzkich zbiorowości. Mimo że włączamy się w jego byt przez uruchomienie środków komunikacji określonego rzędu, ma on charakter permanentny ze względu na skalę konsekwencji oddziaływań. Należy oczekiwać, że fundamentalne instytucje prawne organizujące i urzeczywistniające egzystencję społeczeństw będą ulegać przemianom, których ramy określą nurty ewolucji modelu zbiorowości informacyjnej.

Technologie informacyjne w przestrzeni współczesnych zbiorowości ludzi wywołały potrzebę uruchomienia wielu instytucji, które nie miały dotychczas precedensu w dziejach systemów prawnych, albo przeobraziły instytucje tak bardzo, że stosowanie dotychczasowego opisu doktrynalnego stało się niemożliwe. Najbardziej oczywistymi przykładami są informatyzacja administracji publicznej i idea rządu elektronicznego oraz elektroniczna gospodarka cyfrowa, w której kluczową rolę odgrywają czynności dokonywane przez ludzi w cyberprzestrzeni[28].

Cyberprzestrzeń to miejsce, które pojedynczym osobom i społeczeństwom daje możliwość tworzenia nowych relacji i funkcjonowania. To specyficzna przestrzeń, w której można działać niezależnie od otoczenia, a zasadniczą kwestią cyberprzestrzeni jest informacja.

Za początek społeczeństwa informacyjnego i źródło jego powstania uważa się lata 1956–1957, czyli rozwój gospodarki Stanów Zjednoczonych oraz wstąpienie Japonii do Organizacji Narodów Zjednoczonych (ONZ), a także wystrzelenie w 1956 r. radzieckiego sputnika w kosmos. Zapoczątkowało to erę globalnej komunikacji satelitarnej[29].

Pierwsze wzmianki na temat społeczeństwa informacyjnego pojawiły się w latach 60. XX wieku w Japonii[30]. Pojęcie to zostało użyte po raz pierwszy w 1963 r. przez Tadao Umesao w pracy dotyczącej ewolucyjnej teorii społeczeństwa opartej na informacji[31]. Na początku lat 70. pojęciem tym posługiwał się również Yoneji Masuda w rozważaniach na temat przemian społecznych. Termin „społeczeństwo informacyjne" wiązał się także z rozwojem sektora informacji i telekomunikacji.

W Europie określenie „społeczeństwo informacyjne" wprowadzili dwaj francuscy socjologowie Alain Minc i Simon Nora, którzy użyli go w 1978 r. w raporcie *L'Informatisation de la Société*[32]. Określenie to jednak zawdzięcza popularność Niemcowi Martinowi Bangemannowi, komisarzowi ds. przemysłu, technologii informacyjnych i telekomunikacji, który przygotował raport *Europa a*

społeczeństwo globalnej informacji – zalecenia dla Rady Europejskiej[33]*, potocznie nazywany raportem Bangemanna.*

Plan budowy społeczeństwa informacyjnego w Unii Europejskiej zapoczątkowano w 1993 r. w dokumencie *Growth, Competitiveness and Employment. The Challenges and Ways Forward into 21st Century – White Papier*[34]. Ta *Biała Księga* skoncentrowała się na kwestiach ekonomicznych, a za priorytet przyjęła konkurencyjność gospodarki Wspólnoty Europejskiej oraz osiągnięcie standardów informatycznych wypracowanych przez Stany Zjednoczone. Za początek rozwoju polityki tworzenia społeczeństwa informacyjnego uznaje się jednak wspomniany już dokument *Europa i społeczeństwo globalnej informacji. Zalecenia dla Rady Europy* opublikowany przez Komisję Europejską w 1994 r. W ocenie ekspertów wyrażonej w raporcie społeczeństwo informacyjne powinno się tworzyć, opierając się na finansach sektora prywatnego i mechanizmach rynkowych. Sektor publiczny z kolei powinien pojąć konkretne kroki w celu opracowania odpowiednich regulacji prawnych, ochrony obywateli i konsumentów oraz podnoszenia świadomości społeczeństwa. Postulaty zawarte w raporcie Bangemanna wyznaczyły politykę UE w dziedzinie społeczeństwa informacyjnego.

W roku 1996 Komisja Europejska opublikowała *Green Paper. Living and Working in Information Society. People First*[35]. *Zielona Księga* skupiała się na konsekwencjach, jakie przyniesie dla obywateli transformacja w kierunku społeczeństwa informacyjnego, oraz na wpływie technologii informacyjno-komunikacyjnych (ICT) na jego życie. Kolejną inicjatywą Unii Europejskiej zmierzającą do budowy nowoczesnej i silnej gospodarki krajów członkowskich był projekt *eEurope – An Information Society for All*[36]. Projekt ten opierał się na kilku priorytetach: edukacji, sektorze zdrowia, aktywizacji zawodowej osób niepełnosprawnych i transporcie. W 1999 r. wydano *Green Paper. Public Sector Information: a Key Resource for Europe*. Ta kolejna *Zielona Księga* opisuje korzyści zarówno dla obywateli, jak i całej gospodarki, które wynikają z wykorzystania w obszarze służb publicznych technologii telekomunikacyjnych i informatycznych[37].

Podczas szczytu europejskiego w Santa Maria da Feira w 2000 r. został przyjęty następny plan *eEurope 2002 – An Information Society for All*. Dokument ten wskazywał na konieczność rozwoju szybkiego, taniego, powszechnego Internetu, inwestowania w potencjał ludzki oraz popularyzacji korzystania z sieci wirtualnej. Kolejny plan rozwoju społeczeństwa informacyjnego, rozumianego jako strategiczny element budowy gospodarki opartej na wiedzy, przedstawiono w Göteborgu w 2001 r. W dokumencie *eEurope + 2003: A Cooperative Effort to Implement the Information Society in Europe – Action Plan* założono przyśpieszenie reform i pobudzenie modernizacji gospodarek państw kandydujących do UE przez wykorzystanie narzędzi i technologii społeczeństwa informacyjnego. Do głównych celów należała też poprawa konkurencyjności i spójności społecznej. Inicjatywę tę poparły również kraje kandydujące w tym czasie do Unii Europejskiej.

21–22 czerwca 2002 r. odbył się szczyt UE w Sewilli, podczas którego przyjęto plan rozwoju społeczeństwa informacyjnego do 2005 r. W dokumencie *eEurope 2005: An Information Society for All – Action Plan*[38] państwa członkowskie UE zobowiązały się do realizacji następujących zadań:

- rozwoju usług publicznych online,
- rozwoju usług elektronicznych e-administracji, w tym e-learningu i e-zdrowia,
- tworzenia dynamicznego środowiska do rozwoju gospodarki elektronicznej,
- zapewnienia powszechnego dostępu do Internetu szerokopasmowego,
- budowy systemu bezpieczeństwa infrastruktury informacyjnej.

W roku 1999 prof. Hubert Kubicek[39] określił społeczeństwo informacyjne jako formację społeczno-gospodarczą, w której decydującą rolę odgrywają produktywne wykorzystanie informacji oraz intensywna produkcja nakierowana na wiedzę. Według Kubicka społeczeństwo można nazwać informacyjnym wtedy, gdy obywatele intensywnie korzystają z informacji.

Na gruncie polskim także pojawiło się wiele interesujących definicji społeczeństwa informacyjnego. Jedna z nich jest autorstwa Kazimierza Krzysztofka i Marka S. Szczepańskiego. Społeczeństwem informacyjnym nazwali oni społeczeństwo, w którym informacje intensywnie wykorzystuje się w życiu społecznym, kulturalnym, ekonomicznym i politycznym[40].

Daniel Bell sformułował główne cechy społeczeństwa informacyjnego, twierdząc, że charakteryzuje się ono rosnącą dominacją specjalistów i naukowców w układzie zawodowym, sterowanym rozwojem techniki, a wiedza i informacja staną się źródłem strategii i przemian społeczeństwa[41]. W związku z tym Piotr Sienkiewicz zaproponował definicję przekrojową, według której przez społeczeństwo informacyjne „określamy taki system społeczny, ukształtowany w procesie modernizacji, w którym systemy informacyjne i zasoby informacyjne determinują społeczną strukturę zatrudnienia, wzrost zamożności społeczeństwa (dochodu narodowego) oraz stanowią o orientacji cywilizacyjnej”[42].

Konstrukcja współczesnego modelu społeczeństwa informacyjnego, którego niezaprzeczalnym katalizatorem są technologie stosowane podczas komunikacji elektronicznej przybierającej w wyniku konwergencji formę cyfrową, wyzwala potrzebę refleksji nad fenomenem informacji. W znaczeniu ogólnym cyberprzestrzeń oznacza zbiór informacji tworzony za pomocą Internetu, przestrzeń komunikacyjną tworzoną przez system powiązań internetowych, elektroniczne medium sieci komputerowych z komunikacją w trybie online[43].

Należy zgodzić się z Piotrem Delą, że „cyberprzestrzeń to przestrzeń kooperacji międzyludzkich z wykorzystaniem urządzeń elektronicznych do wytwarzania, przechowywania, przekazywania i przetwarzania informacji[44]”. Współdziałanie to może odbywać się w trzech relacjach:

- człowiek–człowiek,
- człowiek–cyberprzestrzeń,
- cyberprzestrzeń–człowiek.

W pierwszej relacji cyberprzestrzeń jest tylko środowiskiem informacyjnym umożliwiającym wymianę informacji między jej użytkownikami. W drugim przypadku cyberprzestrzeń jest środowiskiem, w którym odbiorca i nadawca tworzą własny wirtualny świat, czyli świat wirtualnej rzeczywistości. Trzecia relacja dotyczy wykorzystania sztucznej inteligencji jako elementu cyberprzestrzeni zdolnego do samodzielnego rozwiązywania problemów odnoszących się do użytkowników[45].

Z cyberprzestrzenią jest bezpośrednio związana przestrzeń informacyjna, która jest złożoną całością interakcji, wartości i funkcji łączących światy: realne, wirtualne, indywidualne, społeczne, przeszłe, obecne i przyszłe[46]. To nie tylko narzędzie wymiany informacji między elementami składowymi systemu bezpieczeństwa podmiotu, lecz także odbicie ich wzajemnych powiązań i relacji[47].

Na początku przestrzeń informacyjna obejmowała zasięgiem tylko społeczności lokalne, lecz z upływem czasu, rozwojem struktur społecznych, umiejętnością wykorzystania narzędzi komunikacyjnych zwiększał się obszar jej powiązań. Rozwój informatyki, telekomunikacji i teleinformatyki doprowadził do tego, że obecnie obejmuje ona swoim zasięgiem całą kulę ziemską, skracając czas obiegu informacji do minimum. To cyberprzestrzeń przeobraziła przestrzeń informacyjną, nadając jej globalny charakter.

Cyberprzestrzeń charakteryzuje się nowymi właściwościami. Do najczęściej wymienianych należą:

- funkcjonowanie w tym samym czasie różnych wymiarów istnienia w zależności od układu odniesienia,
- zjawisko ingresu (wstępowania) polegające na tym, że uczestnicy przestrzeni informacyjnej preferują bardziej intensywność chwili, radość korzystania ze świata niż rozwój (progres),
- ograniczone zaangażowanie i lojalność w stosunku do jednej grupy i jej zasobów informacyjnych, brak emocjonalnego utożsamiania się ze zbiorowością oraz obszarem jej egzystencji,

- brak determinacji uwarunkowanej lokalizacją i związanymi z nią ograniczeniami,
- zastąpienie tożsamości osobowej tożsamością projektowaną ukierunkowaną na samozadowolenie i oczekiwania innych uczestników przestrzeni informacyjnej,
- oderwanie świata wartości od miejsca i czasu jego powstania na rzecz przestrzeni wirtualnej,
- komercjalizację i standaryzację kultury informacyjnej,
- zanik klasycznych struktur społecznych[48].

Współcześnie sieć powiązań informacyjnych jest niejednorodna i wielopoziomowa. Ukształtowała się jako zespół instytucji, jednostek organizacyjnych, zasobów i systemów informacyjnych oraz technologii informacyjnych, które warunkują funkcjonowanie określonych stosunków społecznych, politycznych i ekonomicznych. Infrastruktura informacyjna obejmuje instytucje, zasoby i systemy oraz technologie informacyjne, które określają działanie systemów społecznych, politycznych i ekonomicznych. Zadaniem tej infrastruktury jest gromadzenie, przechowywanie, udostępnianie informacji społeczeństwu, gospodarce i działalności politycznej. Wyróżnia się trzy rodzaje infrastruktury informacyjnej:

- infrastrukturę społeczną – kompleks infrastrukturalnych systemów i zasobów informacyjnych obsługujących społeczne funkcje informacji i procesy społeczne;
- infrastrukturę gospodarki – kompleks systemów i zasobów realizujących funkcje ekonomiczne oraz procesy gospodarcze,
- infrastrukturę polityczną – kompleks systemów i zasobów realizujących funkcje obsługujące system polityczny państwa[49].

We współczesnym świecie każde społeczeństwo i każda gospodarka tworzą pewien społeczny porządek informacyjny rozumiany jako kompleks społecznych norm, procesów, systemów i zasobów informacji, zgodnie z którymi funkcjonują społeczeństwa, państwa i gospodarki. Jest on podstawowym składnikiem infrastruktury społecznej państwa oraz ponadpaństwowych i międzynarodowych struktur[50]. Z tego punktu widzenia w ujęciu

ogólnym systemem informacyjnym można nazwać „taki system działania, którego przeznaczeniem jest efektywna realizacja procesów (zadań) informacyjnych”[51].

- W skład systemu informacyjnego wchodzą m.in.:
- system oświaty publicznej,
- system środków masowej informacji (mass media),
- systemy informacji naukowo-technicznej, prawnej i organizacyjnej,
- systemy biblioteczne,
- statystyka publiczna,
- służby i serwisy informacyjne instytucji i organizacji publicznych (administracji rządowej i samorządowej, ubezpieczenia społecznego, pomocy społecznej, biur pracy, wymiaru sprawiedliwości, służb podatkowych i celnych, instytucji samorządu gospodarczego, związków zawodowych, organizacji politycznych i społecznych)[52].

System informacyjny tworzą złożone układy, których celem jest zapewnienie informacji każdemu użytkownikowi, zgodnie z upoważnieniami, jakie posiada. Do czasu wynalezienia komputerów, Internetu i innych sieci teleinformatycznych nie dostrzegano znaczenia roli systemów informacyjnych. Pełną definicję terminu zaproponował Steinmüller, określając system informacyjny jako „system społeczny, który współtworzą elementy przynależne do pięciu klas: dane, metody, technika (wykorzystywana technologia – wyposażenie techniczne), organizacja, ludzie”[53].

Każda społeczność jest zbiorowością komunikującą się, a pojęcia „społeczność” i „komunikowanie” posiadają wspólne źródłosłowie[54]. Nawet najstarsze społeczeństwa musiały się porozumiewać, aby móc sprawnie funkcjonować.

Bezpieczeństwo systemów informacyjnych jest takie jak poziom bezpieczeństwa najsłabszego z systemów. Termin „polityka bezpieczeństwa informacyjnego” oznacza zestaw praw, reguł i doświadczeń ustalających sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonego systemu.

Bezpieczeństwo informacyjne to inaczej bezpieczeństwo informacji i systemów teleinformatycznych rozpatrywane w odniesieniu do instytucji wykorzystującej lub udostępniającej infrastrukturę teleinformatyczną, aby osiągnąć wyznaczone cele[55].

Zarządzanie bezpieczeństwem to proces ciągły i złożony, umożliwiający bezpieczną realizację zadań, do których powołano daną instytucję. Proces ten zachodzi w stale zmieniającym się środowisku, przy występowaniu coraz nowszych form zagrożeń i wyzwań dla instytucji, a także przy szybkim postępie technologicznym. Bezpieczeństwo w ujęciu całościowym powinno obejmować aspekty: organizacyjny, techniczny i prawny[56].

Nowoczesna ochrona informacji to zespół wielu przedsięwzięć ze sobą powiązanych, ukierunkowanych na osiągnięcie zaplanowanego celu. Stanowi jedną z podstawowych potrzeb człowieka, jaką jest bezpieczeństwo[57]. Podstawowe regulacje muszą być osadzone w realiach prawnych. Na tym poziomie są chronione: ciągłość zadań, ciągłość procesów biznesowych, zdolność świadczenia usług, reputacja, działanie zgodne z prawem. Wszystkie przedsięwzięcia mogą być podejmowane wyłącznie w obrębie obowiązującego prawa. Dotyczy to czynności form ochrony fizycznej, technicznego zabezpieczenia i środków organizacyjnych. Ważnym elementem prawnych uregulowań problemów bezpieczeństwa są przepisy dotyczące ubezpieczenia osób i mienia. Ponieważ uzyskanie absolutnego bezpieczeństwa systemu informacyjnego jest niemożliwe, analiza ryzyka powinna zapewnić stopień bezpieczeństwa proporcjonalny zarówno do wagi chronionej informacji, jak i ilości zastosowanych środków ochrony. Do właściwego zaprojektowania, utworzenia i eksploatacji kompleksowego systemu zabezpieczeń konieczna jest pełna znajomość obiektu chronionego. System informacyjny jest bezpieczny, jeśli jego użytkownik może na nim polegać i działa zgodnie ze stawianymi mu oczekiwaniami. Uważa się, że jest w pełni zabezpieczony, jeżeli istnieje zabezpieczenie dla każdej znanej ścieżki penetracji, czyli każdego zbioru miejsc wrażliwych na atak.

Należy podkreślić, że najsłabszym ogniwem każdego systemu zabezpieczeń jest człowiek. W trosce o bezpieczeństwo przetwarzania danych i ogólne bezpieczeństwo systemów komputerowych należy pamiętać, że wszystkie informacje i wszystkie urządzenia powinny mieć przypisanego właściciela, aby mogły być skutecznie chronione. Właściciel to osoba odpowiedzialna za informacje, za ich kopiowanie, niszczenie, archiwizowanie i inne aspekty przetwarzania i ochrony. Jest to również osoba, która ma uprawnienia pozwalające jej udzielać dostępu do informacji. Bezpieczeństwo informacyjne osiąga się w znacznym stopniu przez realizowanie odpowiednich przedsięwzięć obejmujących środki fizyczne, organizacyjne, osobowe i techniczne[58].

Według normy PN-ISO/IEC 17799:2007 bezpieczeństwo informacji oznacza jej ochronę przed wszelkimi zagrożeniami, która ma na celu zapewnienie ciągłości działania, minimalizacji ryzyka i maksymalizacji zwrotu z inwestycji. Uogólniając, należy stwierdzić, że bezpieczeństwo informacji to wysoki poziom poufności, dostępności i integralności danych będących w posiadaniu danego podmiotu[59].

Bezpieczeństwo informacji jest procesem ciągłym, podczas którego prowadzone są działania zapewniające poczucie bezpieczeństwa Unii Europejskiej. Działania te są zadaniami złożonymi i kosztownymi, dlatego często są argumentem do ich zaniechania. Zarządzanie bezpieczeństwem informacji ma na celu niedopuszczenie do jej ujawnienia. W ogólnym ujęciu rozumiane jest jako stan wolny od zagrożeń dotyczących:

- przekazywania informacji nieuprawnionym podmiotom,
- szpiegostwa,
- działalności dywersyjnej,
- działalności sabotażowej[60].

1.2
ISTOTA BEZPIECZEŃSTWA INFORMACYJNEGO

W UNII EUROPEJSKIEJ

W erze społeczeństwa informacyjnego zapewnienie bezpieczeństwa informacyjnego nabiera szczególnego znaczenia. Jest ono rozumiane jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania. W związku z tym środki ochronne i zabezpieczające podejmowane są w celu zapewnienia poufności, integralności i dostępności informacji oraz wyeliminowania wszelkich potencjalnych zagrożeń. Wśród nich można wyszczególnić środki organizacyjno-proceduralne, personalne, fizyczne czy techniczne (nastawione na ochronę kryptograficzną, elektromagnetyczną, programową, transmisji informacji oraz techniczne wsparcie ochrony fizycznej). Konstruowany system ochrony informacji obejmuje takie obszary funkcjonalne, jak bezpieczeństwo fizyczne, zabezpieczenie procesu przetwarzania informacji, zabezpieczenie sprzętu, zabezpieczenie dostępu do systemu informatycznego, zabezpieczenie procesu wymiany informacji oraz audyt bezpieczeństwa informacji. Wszelka informacja istnieje w społeczeństwie zawsze w ramach określonego procesu informacyjnego, przez który można rozumieć swoisty proces technologicznego funkcjonowania informacji. Składają się na niego następujące operacje: generowanie, gromadzenie, przechowywanie, przekazywanie, przetwarzanie, udostępnianie, interpretacja i wykorzystanie informacji[61]. Bezpieczeństwo informacyjne odnosi się do każdej z tych operacji. Właśnie to pozwala jednoznacznie odróżnić bezpieczeństwo informacji od bezpieczeństwa informacyjnego jako bezpieczeństwo przedmiotu, obiektu i procesu[62].

Bezpieczeństwo informacji kategoryzują takie właściwości, jak poufność (informacja nie jest udostępniana lub ujawniana podmiotom nieuprawnionym), integralność danych (nie są zamieniane lub niszczone w sposób nieautoryzowany) czy systemu (system realizuje swoje funkcje w sposób nienaruszony, wolny od nieautoryzowanej manipulacji), dostępność (zapewnienie

możliwości autoryzowanego wykorzystania danych w założonym czasie), autentyczność (zgodna z zadeklarowaniem tożsamość podmiotu lub zasobu), rozliczalność (jednoznaczne przypisanie działania podmiotu tyko temu podmiotowi), niezawodność (spójne, zamierzone zachowania i skutki)[63]. Bezpieczeństwo informacyjne nie dotyczy wyłącznie informacji, a obejmuje również systemy, w których jest ona wytwarzana, przetwarzana, przechowywana czy przekazywana, oraz środowisko, w którym te systemy działają, personelu, który korzysta z tych systemów (i który często bywa niedouczony, nieobliczalny w swoich reakcjach i trudny do skontrolowania), a także całego otoczenia formalnoprawnego, które kształtuje zarówno technologie informacyjne, jak i procesy użytkowania informacji.

W strukturze bezpieczeństwa informacyjnego można wyróżnić takie elementy, jak zasoby (materialne i niematerialne), zagrożenia (zamierzone lub przypadkowe) ze strony ludzi lub środowiska, podatność (słabe strony systemu), następstwa ryzyka (uświadamianie użytkowników o zagrożeniach) czy różnego rodzaju ograniczenia (np. finansowe, techniczne, organizacyjne, prawne). Z wyrywkowo dokonanego przeglądu wynika, że bezpieczeństwo jest zjawiskiem multigatunkowym, wielowymiarowym, wielopłaszczyznowym, wieloaspektowym, o różnym stopniu złożoności, stąd mnogość różnych klasyfikacji.

Pozostając przy stanowisku, że zasadniczą linię podziału tworzy dychotomia – bezpieczeństwo podmiotowe bądź przedmiotowe, a zarazem czerpiąc inspiracje z wiedzy antropologicznej czy ekokulturowej, spróbujmy spojrzeć na dotychczasowe kategorie bezpieczeństwa w nieco inny sposób. W odniesieniu do wymiaru podmiotowego można zaproponować dodanie typologii bezpieczeństwa terytorialno-przestrzennego (obejmującego agregaty podmiotów bezpieczeństwa sytuujących się w ściśle zakreślonej przestrzeni ich naturalnego występowania), a zarazem doprecyzować typologię bezpieczeństwa stricte podmiotowego.

W takim ujęciu właściwe bezpieczeństwo podmiotowe obejmowałoby następujące wymiary:

- podmiotowo-personalny (pojedyncza osoba, jednostka gatunku ludzkiego),
- podmiotowo-wspólnotowy (np. UE, NATO, grupa społeczna – rodzina, naród, społeczeństwo),
- podmiotowo-instytucjonalny (struktury społeczne – przedsiębiorstwo, organizacja społeczna, państwo, koalicja państw itp.).

Z kolei na bezpieczeństwo podmiotowe z uwzględnieniem usytuowania terytorialno-przestrzennego, czyli bezpieczeństwo podmiotowo-terytorialno-przestrzenne (które *de facto* odnosi się nie do parametrów fizyko-geograficznych, ale do podmiotów ludzkich sytuujących się akurat w danej przestrzeni), składają się:

- bezpieczeństwo powszechne,
- bezpieczeństwo publiczne,
- bezpieczeństwo lokalne,
- bezpieczeństwo międzynarodowe (nie w odniesieniu do struktur międzynarodowych swoistych podmiotów, jak np. UE, lecz w sensie bezpieczeństwa w określonym regionie świata, czyli w relacjach międzypaństwowych),
- bezpieczeństwo globalne itp.

Nieco mniejsze pole manewru na modyfikację pozostawia kryterium przedmiotowe. Tu jednak również można wskazać możliwości nowego pogrupowania. Można tu mówić o bezpieczeństwie w ogólnych płaszczyznach (przestrzeniach, dziedzinach) życia, funkcjonowania jednostkowego bądź społecznego, a zatem o bezpieczeństwie: politycznym, wojskowym (czy militarnym), gospodarczym (ekonomicznym), społecznym, kulturowym, ideologicznym, ekologicznym, informacyjnym, zdrowotnym, socjalnym, zawodowym, interpersonalnym, komunikacyjnym itp. Ponadto można przedmiotowo klasyfikować bezpieczeństwo według konkretnych kategorii aktywności ludzkiej i przykładowo w odniesieniu do danej jednostki mówić o bezpieczeństwie: jej snu, zabawy, pracy, konsumpcji, seksu, przemieszczania się itp. To różnica nie tylko werbalna, lecz także

substancjonalna. Tak zarysowane kategorie bezpieczeństwa stanowią przedmiot zainteresowania nauk społecznych, a co za tym idzie również nauk o bezpieczeństwie. Przedstawioną propozycję rekonstrukcji typologii bezpieczeństwa można przy tym potraktować jako element rozwijanej w dalszej części refleksji nad możliwościami doskonalenia paradygmatu bezpieczeństwa w perspektywie jego ogólnej teorii, coraz intensywniej rozwijającej się w ostatnich czasach[64].

Polityka bezpieczeństwa informacyjnego ma na celu zapewnienie stabilnej pracy systemu informacyjnego, poufności przetwarzania informacji, ochronę przed modyfikacją oraz ograniczenie do minimum ryzyka przeprowadzenia ataku na system informacyjny. Polityka bezpieczeństwa informacyjnego obejmuje cały proces korzystania z informacji, niezależnie od metodyki jej przetwarzania (tj. zbierania, gromadzenia, opracowywania, aktualizacji, udostępniania i usuwania). Dotyczy wszystkich systemów przetwarzania danych i informacji, zarówno systemów prowadzonych tradycyjnie (dokumenty papierowe, różnego typu archiwa, kartoteki), jak i systemów teleinformatycznych. W praktyce można spotkać wiele technik, metod i narzędzi, bardziej i mniej skutecznych tworzenia polityki bezpieczeństwa informacji[65].

Polityka cyberbezpieczeństwa definiuje sposoby korzystania z kont użytkowników i danych przechowywanych w systemie, zapewniając właściwą ochronę informacji instytucji. W każdej organizacji są informacje chronione, np. dane osobowe, informacje finansowe, oraz informacje jawne, w tym informacje marketingowe. Dlatego też przedmiotem polityki bezpieczeństwa UE jest również informacja znajdująca się w systemie teleinformatycznym. Celem polityki bezpieczeństwa informacyjnego jest opracowanie procedur i wymagań niezbędnych do zapewnienia właściwej ochrony informacji w Unii. Używając pojęcia polityki cyberbezpieczeństwa, ustala się zbiór praw, reguł i wskazówek praktycznych, które określają takie kwestie, jak zasoby teleinformatyczne, w tym informacje wrażliwe, które są zarządzane, chronione i dystrybuowane w Unii Europejskiej

i państwach członkowskich, w ich systemach teleinformatycznych. Ochronie na tym poziomie podlegają:

- zasoby informacji,
- oprogramowanie,
- sprzęt,
- kadry,
- dokumenty[66].

Polityka bezpieczeństwa informacyjnego obejmuje również sprzęt i oprogramowanie, za pomocą których informacje są przetwarzane, oraz ludzi przetwarzających te informacje. Każda organizacja ma swoją specyfikę i powinna mieć odrębną politykę bezpieczeństwa[67]. Nie można zakładać, że raz opracowana polityka bezpieczeństwa organizacji będzie w niej zawsze funkcjonowała poprawnie. Unia zmienia się w czasie zarówno jako organizacja, jak i struktura, system teleinformatyczny także ulega ewolucji, dlatego też polityka bezpieczeństwa informacyjnego powinna być ciągle dostosowywana do zmieniających się warunków wewnętrznych i zewnętrznych UE. Niemniej jednak można wskazać typowe elementy, które powinna posiadać każda polityka bezpieczeństwa systemu informacyjnego[68].

Europejska dyskusja, która toczy się wokół kwestii związanych z ochroną danych i bezpieczeństwem informacyjnym, daleko odeszła od pierwotnej intencji, jaką było ustanowienie barier i ograniczeń dla działań inwigilacyjnych państwa wobec własnych obywateli, co stało się możliwe z chwilą rozwoju i upowszechnienia komputerów i Internetu. Z jednej strony uznano bowiem za oczywiste, że naruszenie zadeklarowanych praw obywateli związanych z bezpieczeństwem ich danych i ochroną ich prywatności nie musi odbywać się przy użyciu komputerów i systemów komunikacji elektronicznej, ale może również dotyczyć tradycyjnych analogowych sposobów gromadzenia i przetwarzania danych. Z drugiej – zauważono coraz większy wzrost aktywności podmiotów biznesu prywatnego na tym polu i zdano sobie sprawę, że w wielu sytuacjach pozyskiwanie, gromadzenie, przetwarzanie, przechowywanie i udostępnianie osobom trzecim danych obywateli

w celach komercyjnych stanowi dla osób zainteresowanych większe zagrożenie niż działania inwigilacyjne państwa powodowane względami bezpieczeństwa czy racjonalizacji polityki. Dlatego w toczącej się dyskusji polityczno-prawnej wokół zagadnień bezpieczeństwa danych i ochrony prywatności środek ciężkości coraz bardziej przesuwa się w kierunku komercyjnego wykorzystania danych związanych np. z rejestracją i obsługą klientów czy problemów wynikających z postępowania pracodawcy z danymi pracowników. W rezultacie prowadzonych debat kwestie ochrony danych od lat 70. XX wieku zaczęły nabierać coraz większego znaczenia politycznego i wzbudzać coraz większe zainteresowanie społeczne, czego wyrazem było wdrożenie prawnych standardów ochrony danych osobowych i utworzenie w większości państw na świecie instytucji nadzoru nad ich przestrzeganiem[69].

Przełomem było wydanie przez Unię Europejską w 1995 r. *Dyrektywy w sprawie ochrony danych*[70], która nie tylko nakładała na państwa członkowskie obowiązek odpowiedniego dopasowania krajowego ustawodawstwa do europejskich standardów, lecz także za sprawą przepisów regulujących transfer danych z obszaru Unii Europejskiej do państw trzecich wywarła presję legislacyjną na wiele pozaeuropejskich państw i skłoniła je do przyjęcia podobnych rozwiązań prawnych, które ułatwiły wymianę handlową z UE. Fundamentem prawa unijnego stały się te same zasady, na których opierała się amerykańska ustawa o prywatności: legalność i uczciwość w pozyskiwaniu danych, ograniczanie się jedynie do tych danych, które są absolutnie niezbędne, przetwarzanie danych tylko w ściśle określonym celu, informowanie zainteresowanych i uzyskiwanie ich zgody oraz – co dla wielu najważniejsze – zapewnienie zainteresowanym prawa do wglądu w swoje dane. Dzięki nagłaśnianiu kwestii ochrony danych pozyskiwanie, zapisywanie i przetwarzanie danych osobowych, a w jeszcze większym stopniu ich udostępnianie osobom postronnym bez wiedzy i wbrew woli osób, których te dane dotyczą, powszechnie uważa się dzisiaj za formę naruszenia praw człowieka i obywatela podobną do zamachu na inne podstawowe dobra ludzkie chronione

prawem, takie jak życie, zdrowie, własność czy wolność. Uważa się za oczywiste, że każde naruszenie praw podstawowych wymaga potwierdzenia w legislacji.

Działania Unii Europejskiej, jako jedynej obecnie organizacji międzynarodowej, wyraźnie zmierzają do wzmocnienia ochrony prywatności osób korzystających z elektronicznych systemów komunikacyjnych i informacyjnych. W tym celu UE bierze „pod lupę" dostawców usług z sektora łączności, w szczególności operatorów takich komunikatorów, jak Facebook Messenger, WhatsApp czy Skype. Proponowane nowe rozporządzenie w sprawie ochrony prywatności w komunikacji elektronicznej zaktualizuje i rozszerza dotychczas obowiązujące przepisy oraz dostosowuje je do ogólnego rozporządzenia o ochronie danych[71]. Ochrona poufności danych dotyczyć ma zarówno treści rozmów i danych zawartych w korespondencji elektronicznej, jak i metadanych odnoszących się do daty i czasu trwania połączeń, a także informacji wykorzystywanych dotychczas do tworzenia spersonalizowanych rejestrów usług oraz profilowania klientów i użytkowników, takich jak zainteresowania i preferencje związane z wyszukiwaniem informacji i przeglądaniem stron www, a nawet sposoby klikania w przyciski. Korzystanie ze wszystkich danych zapisanych na urządzeniu klienta, podobnie jak śledzenie zachowań użytkowników w Internecie za pomocą tzw. ciasteczek lub innych technologii, będzie wymagało uzyskania wyraźnej zgody użytkownika. Co w przygotowywanych przepisach jest przełomowe – taka zgoda nie będzie mogła być wymuszana groźbą odmowy dostępu do serwisu lub świadczenia usługi, tak jak to się dzieje obecnie. Firmom będzie wolno korzystać bez ograniczeń jedynie z takich ciasteczek, które nie ingerują w prywatność użytkownika. Specjalna zgoda nie będzie wymagana do korzystania z ciasteczek, których celem jest np. liczenie osób odwiedzających daną stronę internetową, zapamiętywanie danych logowania lub zawartości koszyka.

Prawo do ochrony danych stanowi nieodłączną część systemu praw podstawowych UE. Z wielu stron zgłaszane są jednak wątpliwości dotyczące tego, że amerykańskie firmy i ich partnerzy

pomagają służbom USA w działaniach szpiegowskich naruszających europejskie prawa podstawowe. Ograniczenia w międzynarodowym transferze danych i w dostępie do prywatności nie wszystkim – rzecz jasna – się podobają. Amerykańska Fundacja na rzecz Technologii Informacyjnej i Innowacyjności (ITIF) uznała zerwanie porozumienia z 7.10.2015 r. między USA a UE i Szwajcarią w sprawie bezpiecznej przystani dla danych za katastrofę dla transatlantyckiej gospodarki cyfrowej i porównała je z przecięciem wszystkich podmorskich światłowodów łączących oba kontynenty[72].

W takim stwierdzeniu jest sporo przesady. Z całą pewnością jesienią 2015 r. nie doszło do nagłego wstrzymania eksportu danych osobowych z Europy do Stanów Zjednoczonych. Mimo stwierdzenia nieważności porozumienia o bezpiecznej przystani dane klientów europejskich nadal są przesyłane do USA, jeśli tylko zainteresowani wyrażą na to zgodę albo taka konieczność wynika z realizacji zawartej umowy. Można również założyć, że wiele firm ignoruje fakt unieważnienia porozumienia *Safe Harbor* i w swoich praktykach związanych z operacjami z użyciem danych osobowych nadal daleko wykracza poza standardy ochrony prywatności obowiązujące w Europie w nadziei, że sprawa nigdy nie trafi do sądu. Trwają prace nad tzw. porozumieniem parasolowym, które ma ujednolicić standardy w zakresie ochrony danych dotyczące wszystkich mechanizmów przekazywania danych. Niezadowolenie gigantów internetowych, którym wysokie standardy zabezpieczenia prywatności w Europie psują interesy, jest jednak zrozumiałe.

Obok państwowych ustawodawstw z zakresu ochrony danych od początku lat 80. XX wieku pojawiło się także wiele regulacji międzynarodowych, o mniej lub bardziej wiążącym charakterze, odnoszących się do postępowania z danymi dotyczącymi osób zarówno na poziomie krajów, jak i w relacjach międzynarodowych. Europejska Organizacja Współpracy i Rozwoju (OECD) wydała np. w 1980 r. niewiążące *Wytyczne dotyczące ochrony prywatności i transgranicznego przepływu danych osobowych*[73], a rok później Rada Europy uchwaliła *Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych*[74] prawnie wiążącą

dla państw członkowskich. Jednak tak naprawdę pierwszym „twardym" dokumentem prawa międzynarodowego regulującym kwestie ochrony prywatności i bezpieczeństwa danych w Europie była *Dyrektywa w sprawie ochrony danych* z 1995 r.[75] Ujednolicała ona standardy postępowania z danymi spersonalizowanymi dotyczącymi osób na poziomie kontynentalnym. Nie jest jednak do końca jasne, co motywowało pomysłodawców dyrektywy i ostatecznie przesądziło o podjęciu działań harmonizujących ustawodawstwo w zakresie ochrony danych na szczeblu unijnym: interesy związane z prawami i bezpieczeństwem obywateli czy przesłanki biznesowe. Jak się szybko okazało, regulacje ułatwiły przede wszystkim przeprowadzanie międzynarodowych operacji firmom uzależnionym w swojej działalności od wykorzystywania danych osobowych.

Wytyczna, zobowiązując wszystkie kraje członkowskie do uzgodnienia krajowych przepisów z nowymi europejskimi standardami, pozostawiała państwom sporo swobody w działaniach dostosowawczych, zabraniając transferowania danych do krajów trzecich, w których nie obowiązują te same standardy ochrony danych, nałożyła obowiązek zawierania z krajami spoza Wspólnoty, w tym z jej największymi partnerami handlowymi: USA, Rosją i Chinami, odrębnych umów w zakresie ochrony danych. W praktyce jednak umowy takie często były nieskuteczne, jak pokazuje przykład programu *Safe Harbor*[76] uregulowanego umową między Komisją Europejską a Departamentem Handlu USA zawartą w 2000 r. w kontekście działalności demaskatorskiej Edwarda Snowdena, a szczególnie w kontekście orzeczenia Trybunału Europejskiego stwierdzającego na wniosek Komisji Europejskiej nieważność tej umowy[77].

Ponieważ wytyczna unijna z 1995 r. odnosiła się do ówczesnej sytuacji związanej z upowszechnieniem komputerów PC, nastanie ery Internetu na przełomie drugiego i trzeciego tysiąclecia wymusiło gruntowne zmiany uregulowań w obszarze ochrony danych. Reagując na nową sytuację, Unia Europejska wydała w 2002 r. dyrektywę o ochronie danych i komunikacji elektronicznej *ePrivacy Directive*[78], którą w 2009 r. znowelizowała w formie tzw. dyrektywy

ciasteczkowej[79]. Ostatnim znaczącym aktem mocującym ochronę danych i prawo do prywatności w ustawodawstwie europejskim było wpisanie zarówno zasady poszanowania życia prywatnego i życia rodzinnego (art. 7), jak i zasady ochrony danych osobowych (art. 8) do *Karty praw podstawowych Unii Europejskiej*[80].

W związku z postępującym rozwojem komunikacji elektronicznej od 2012 r. europejskie ustawodawstwo w zakresie ochrony danych znajduje się w fazie permanentnych, gruntownych transformacji, czego przykładem jest unijny pakiet reform z 2012 r. składający się z ogólnego rozporządzenia o ochronie danych[81], mającego moc prawa wspólnotowego, oraz dyrektywy w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych[82], która ma charakter ramowych wytycznych regulujących sposób postępowania z danymi osób przez organy wymiaru sprawiedliwości i policji wymagających dopiero wdrożenia do systemów prawnych poszczególnych państw członkowskich. Pracom nad wspomnianym pakietem reform towarzyszyły zarówno silne naciski ze strony elit politycznych, jak i agresywny lobbing wielkich korporacji[83]. Stawką w grze były bowiem przepisy regulujące możliwości wykorzystywania jednego z najważniejszych obecnie zasobów, jakim jest informacja, i będące istotnym czynnikiem dalszych przemian europejskiego modelu społeczeństwa informacyjnego.

Należy zwrócić uwagę na często poruszany w literaturze przedmiotu i nadal poddawany dyskusji problem charakteru prawnego poczty elektronicznej i prawidłowej kwalifikacji adresu e-mail jako jednej z postaci danych osobowych[84]. Zgodnie ze stanowiskiem Generalnego Inspektora Ochrony Danych Osobowych adres poczty elektronicznej należy do kategorii danych osobowych tylko wówczas, gdy zawiera informacje o imieniu i nazwisku użytkownika lub inne podobne informacje. Można też przyjąć, że o statusie adresu poczty elektronicznej rozstrzyga treść identyfikatora i domeny oraz powiązanie adresu e-mail z innymi danymi pozwalającymi na identyfikację osoby, lub bronić stanowiska, zgodnie z którym skoro wiadomość dociera do odbiorcy po adresie e-

mailowym, to znaczy, że można go zidentyfikować właśnie przez ten adres[85].

Niewątpliwie za słuszne należy uznać twierdzenie, że nie ma przeszkód, aby za informację umożliwiającą zidentyfikowanie konkretnej osoby uznać adres e-mail, a w związku z tym możliwa jest kwalifikacja adresów e-mailowych jako danych osobowych podlegających ochronie. Należy jednak mieć na względzie to, że jednak nie każdy adres poczty elektronicznej daje możliwość szybkiej i bezproblemowej identyfikacji osoby, do której jest przypisany, a zgodnie z powołanymi wcześniej postanowieniami ustawy o ochronie danych osobowych proces ustalania tożsamości osoby, do której przypisany jest konkretny adres e-mail, nie może być procesem długotrwałym, skomplikowanym i kosztownym.

Wszystkie wymienione próby uregulowania kwestii ochrony danych i ochrony prywatności próbowały wzajemnie zbalansować przeciwstawne interesy, które logicznie są nie do pogodzenia: interesy osób fizycznych związane z poszanowaniem ich prywatności i interesy biznesu związane z możliwie nieograniczonym dysponowaniem informacjami o tych osobach. W obliczu tych konfliktów interesów w polityce ochrony danych i ochrony prywatności jest również wiele przeciwstawnych stanowisk i wizji, choć granice między poszczególnymi stanowiskami często się zacierają. Jeśli chodzi o szeroko rozumiane interesy ekonomiczne, to z jednej strony mamy do czynienia z przedsiębiorstwami kierującymi się motywami komercyjnymi, z drugiej zaś – z aktorami z obszaru polityki gospodarczej, takimi jak ministerstwa gospodarki, którym zależy np. na tworzeniu nowych miejsc pracy. Obie strony mogą w odniesieniu do Internetu preferować klasyczny rynkowy liberalizm oparty na zasadzie minimalizacji kosztów transakcyjnych i ograniczonej ingerencji regulacyjnej państwa. Z punktu widzenia takiego stanowiska ochrona danych w Internecie byłaby czynnikiem dodatkowo podnoszącym koszty transakcyjne, co paradoksalnie ułatwiałoby firmom wymuszanie lojalności klientów. Niezależnie od konkretnych rozwiązań przyjętych w poszczególnych państwach ochrona danych jako taka stanowi obszar międzyresortowy o niezbyt

spójnych, całościowych i wypełniających uregulowaniach oraz o bliżej nieokreślonym podziale i przydziale kompetencji, leżący „w poprzek" tradycyjnych politycznych rozgraniczeń na bezpieczeństwo wewnętrzne i administrację, obronę narodową, politykę zagraniczną i politykę gospodarczą.

Z historycznego punktu widzenia ochrony danych nie można traktować jedynie jako zbioru uprawnień służących ochronie obywateli przed ingerencją organów państwa i podmiotów z sektora biznesu w sferę ich prywatności. Ochronę danych należy rozumieć o wiele szerzej jako zespół praw związanych z informacyjnym samookreśleniem, obejmujących przede wszystkim poszanowanie prawa obywatela do współdecydowania i uczestnictwa w publicznych procesach decyzyjnych oraz wielu innych praw podstawowych.

Szczególną aktywność we wpływaniu na ostateczny kształt zapisów w wymienionych dokumentach wykazywały czołowe amerykańskie spółki z branży IT[86], o czym najdobitniej świadczą przecieki z posiedzeń Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) Parlamentu Europejskiego donoszące, że w poprawkach zgłaszanych przez eurodeputowanych z tej komisji znajdowały się duże fragmenty tekstu skopiowane ze stanowisk czołowych koncernów przedłożonych w trakcie konsultacji z kluczowymi interesariuszami[87]. Mimo desperackich działań lobbystów, podejmowanych w celu przewlekania prac nad ogólnym rozporządzeniem unijnym o ochronie danych (m.in. poddano pod głosowanie ponad 4000 propozycji poprawek), ostatecznie LIBE jesienią 2013 r. osiągnęła kompromis w sprawie ostatecznego kształtu tego dokumentu i skierowała go do Parlamentu Europejskiego, a ten wiosną 2014 r. uchwalił rozporządzenie w trakcie pierwszego czytania przytłaczającą większością głosów. Z pewnością mobilizująco na europarlamentarzystów podziałał skandal inwigilacyjny związany z programem PRISM, ujawniony w czerwcu 2013 r. przez Edwarda Snowdena.

O ile przyjęcie pakietu reform na poziomie Parlamentu Europejskiego wymagało jedynie dwóch lat prac legislacyjnych i

osiągnięcie większościowego kompromisu okazało się zaskakująco łatwe, o tyle podjęcie decyzji na szczeblu Rady Europejskiej wymagało twardych negocjacji i złamania oporu rządów wpływowych krajów sprzeciwiających się regulacjom ograniczającym swobodę działania organów państwa (głównie Niemcy) albo przeregulowaniu sektora prywatnego biznesu (głównie Wielka Brytania)[88]. Wiosną 2015 r. europejska internetowa platforma demaskatorska przeciwdziałająca pladze lobbingu upubliczniła ponad 10 tys. wewnętrznych dokumentów unijnej rady ministrów, które dają ponury obraz przebiegu negocjacji towarzyszących wdrażaniu rozporządzenia parlamentu w sprawie ochrony danych i świadectwo niezbyt konstruktywnych działań podejmowanych przez przedstawicielstwa poszczególnych państw członkowskich. Zwłaszcza zgłaszane bez końca przez przedstawicieli niemieckiego Federalnego Ministerstwa Spraw Wewnętrznych propozycje poprawek były korzystne dla interesów bezpieczeństwa państwa, a przy okazji również dla wielkich korporacji[89].

* * *

Podsumowując, należy stwierdzić, że cyberterroryzm i zagrożenia z nim związane mają charakter asymetryczny i ponadnarodowy. Przeciwdziałanie zjawisku nie jest zagadnieniem prostym, ponieważ należy prowadzić działania systemowe na wielu płaszczyznach. Jest wiele powodów, dla których przeciwdziałanie cyberterroryzmowi napotyka wiele przeszkód, m.in. niepaństwowy charakter, niebezpośredniość ataku, prowadzenie ataku na odległość, możliwość rozłożenia go w czasie, łatwość przeprowadzenia ataku, konieczność nieustannego dopracowywania rozwiązań formalnoprawnych służących przeciwdziałaniu cyberterroryzmowi. Aktów cyberterroryzmu można dokonać małym kosztem, wystarczą bowiem laptop i dostęp do Internetu. Korzystanie przez terrorystów z elektronicznych kanałów porozumiewania się na odległość może dawać wrażenie anonimowości i niemożności ich wykrycia. Jest to jednak mylne przekonanie. Niemal każda działalność w sieci pozostawia cyfrowy „ślad”. Służby wywiadowcze państw stale

prowadzają działania w celu zbierania takich dowodów, wykrywania sprawców i zapobiegania atakom.

Cyberterroryzm jest jednym z zagrożeń hybrydowych, którego celem jest nie tylko spowodowanie bezpośrednich szkód i wykorzystanie słabości, lecz także destabilizacja społeczeństwa. Zagrożenie to jest coraz bardziej realne. Od 2015 r. ISIS intensywnie dokonuje ataków cyberterrorystycznych w Europie. Terroryści zrozumieli, że przestrzeń wirtualna ma gigantyczny wpływ na opinię publiczną, a treści publikowane w Internecie mogą być narzędziem dodatkowym.

Wymiar i charakter zagrożenia były czynnikami wyzwalającymi przygotowanie polityki ochrony cyberprzestrzeni, która ewoluuje i zmierza do harmonizacji norm prawnych przyjętych w prawie UE, chociaż proces ten postępuje z różną szybkością w poszczególnych państwach członkowskich i nie należy go uznawać za zakończony. W ostatnich latach, gdy cyberprzestrzeń ulegała coraz większemu zmilitaryzowaniu, zaczęła być postrzegana jako piąta dziedzina działań wojennych, ponieważ cyberobrona chroni systemy, sieci i infrastrukturę krytyczną wojska w cyberprzestrzeni przed atakami.

Zarządzanie bezpieczeństwem informacji polega na wdrażaniu struktur i polityk oraz zapewnieniu poufności, integralności i dostępności danych. Częścią tego procesu jest zarządzanie cyberbezpieczeństwem. Dotyczy to zagrożeń cybernetycznych ze wszystkimi ich typami, które są nieraz trudne do wykrycia lub zarządzania nimi. Modele zarządzania cyberbezpieczeństwem różnią się w poszczególnych państwach członkowskich. Odpowiedzialność za cyberbezpieczeństwo jest często podzielona na wiele podmiotów. Te różnice mogą utrudniać współpracę potrzebną do reagowania na incydenty graniczne zakrojone na szeroką skalę i na wymianę informacji o zagrożeniach na szczeblach krajowym i unijnym.

Dążenie do osiągnięcia przez Unię Europejską niezależności strategicznej w cyberprzestrzeni nie jest oparte na wystarczających podstawach prawnych i w dużym stopniu zależy od dysponowania własnymi zdolnościami do cyberobrony. Państwa członkowskie dostrzegają potrzebę wzmocnienia posiadanych zasobów, jednak niechętnie podchodzą do udostępniania własnych zdolności w tym

zakresie. Potencjał państw w dziedzinie cyberbezpieczeństwa jest mocno zróżnicowany. Wystąpienie Wielkiej Brytanii z Unii znacząco osłabia jej potencjał w tej kwestii. Brytyjczycy posiadają dużo różnych zdolności cybernetycznych, w tym jako jedni z nielicznych dokonywania ofensywnych i defensywnych cyberataków. Ponadto współpracują w zakresie wywiadu i rozpoznania elektronicznego państw anglosaskich. Konieczność utrzymania bliskiego, zinstytucjonalizowanego współdziałania Wielkiej Brytanii z Unią Europejską w kwestii cyberbezpieczeństwa dostrzegają obie strony, o czym może świadczyć dokument rządu brytyjskiego przedstawiony przed rozpoczęciem negocjacji dotyczących warunków brexitu[90].

2

STRATEGIA CYBERBEZPIECZEŃSTWA UNII EUROPEJSKIEJ W XXI W.

Jedno z podstawowych, a zarazem najtrudniejszych współczesnych zagadnień, z którymi spotykamy się w rzeczywistości społecznej, stanowi formułowanie polityki przez państwo i jej realizacja oparta na strategii. Zasadniczą kwestią jest przy tym sposób organizacji władzy w państwie, unormowania prawne i organizacyjne, które odgrywają kluczową rolę w efektywnym stosowaniu polityki i strategii. Wpływa to na formułowanie i realizację polityki i strategii państwa w podobnym stopniu, jak przygotowanie elit politycznych do sprawowania władzy w państwie. Nie bez znaczenia pozostaje przy tym kontekst historyczny. W związku z tym przedmiotem analizy drugiego rozdziału będzie wyjaśnienie, czym jest strategia bezpieczeństwa UE i jak się zmieniała w czasie. Nie można tego uczynić bez wyjaśnienia, czym jest paradygmat bezpieczeństwa państwa oraz jak ewoluuje. Ma to na celu wykazanie, w jaki sposób polityka i strategia oddziałują na siebie, ze szczególnym uwzględnieniem koncepcji bezpieczeństwa Unii Europejskiej. Rozważania na temat *Europejskiej strategii bezpieczeństwa* ukażą znaczenie strategii bezpieczeństwa jako instrumentu polityki cyberbezpieczeństwa UE. Z kolei analiza ESB przedstawi istotę jej koncepcji, zmiany, jakie nastąpiły przez lata, oraz na czym polega zakres obecnej strategii ochrony UE w cyberprzestrzeni. Zostaną

również przedstawione cechy polistrategii bezpieczeństwa, a połączenie polityki i strategii umożliwi zrozumienie i wyjaśnienie, że to właśnie one określają byt i rozwój państwa, mając jednocześnie zmienny i dynamiczny charakter. Polityka i strategia są warunkowane przez zagrożenia i wyzwania, dlatego można stwierdzić, że umiejętne połączenie polityki i strategii gwarantuje pomyślność działań w każdym z zakresów aktywności państwa, w tym również w obszarze ochrony cyberprzestrzeni.

2.1
PARADYGMAT BEZPIECZEŃSTWA PAŃSTWA W STOSUNKACH MIĘDZYNARODOWYCH

Pojęcie „paradygmat" jest używane w różnych dziedzinach nauki i występuje w odmiennych znaczeniach. *Powszechna encyklopedia filozofii* charakteryzuje paradygmat następująco: „(gr. *paradeigma* – wzór, model; łac. *paradigma* – wzór, przykład) pierwotne określenie idei platońskiej, która stanowiła prawzór rzeczy zmiennych; współcześnie: w językoznawstwie – zespół form deklinacyjnych albo koniugacyjnych właściwych danemu rodzajowi wyrazów; w retoryce – wyjątkowo jasny i typowy przykład ilustrujący omawianą kwestię"[91]. *Encyklopedia PWN* podaje natomiast taką oto definicję[92]: „paradygmat (gr. *parádeigma* – wzór) – ogólnie uznane osiągnięcie naukowe (teoria naukowa), które w pewnym okresie dostarcza modelowych rozwiązań w danej dziedzinie nauki"[93].

Paradygmat w rozumieniu wprowadzonym przez filozofa Thomasa Kuhna w książce *Struktura rewolucji naukowych* opublikowanej w 1962 r. to zbiór pojęć i teorii tworzących podstawy danej nauki, którego raczej się nie kwestionuje, przynajmniej do czasu, kiedy paradygmat jest twórczy poznawczo, tzn. za jego pomocą można konstruować teorie szczegółowe zgodne z danymi doświadczalnymi (historycznymi), którymi zajmuje się dana nauka[94]. Kuhn,

przywołując pojęcie paradygmatu, aby opisać proces rozwoju nauk i dostosować go do tego obszaru, zdecydowanie poszerzył jego pierwotne znaczenie. O paradygmatach pisał, że są to „powszechnie uznawane osiągnięcia naukowe, które w pewnym czasie dostarczają społeczności uczonych modelowych problemów i rozwiązań".

Zatem paradygmat to przede wszystkim uznawana w pewnym czasie teoria bądź teorie naukowe. Z jednej strony funkcjonuje niczym wzorzec odmiany gramatycznej, tj. w tym sensie, że dostarcza modelowych praktyk, które można reprodukować w dalszych badaniach, z drugiej – wyznacza problemy do rozwiązania, a więc określa kształt dalszych badań. Owe badania są związane z procesem uściślania pewnych pojęć i wyciągania z teorii konsekwencji. Pod ich wpływem zmiany zachodzą także w paradygmacie. Ich sygnałem jest pojawienie się pewnych niezgodności, które Kuhn nazywa „anomaliami".

Anomalie oznaczają sytuacje, w których badany przedmiot zachowuje się niezgodnie z przewidywaniami wynikającymi z założeń paradygmatu. W koncepcji paradygmatu Kuhna można zatem wyróżnić trzy główne momenty:

- teorię wraz z praktykami,
- badania nad dookreśleniem teorii i wyciąganiem z niej konsekwencji,
- anomalie.

Kuhn utrzymywał także, że – wbrew obiegowym opiniom – typowi naukowcy nie są obiektywnymi i niezależnymi myślicielami, lecz konserwatystami, którzy godzą się z tym, czego ich nauczono, i stosują tę naukę (wiedzę) do rozwiązywania problemów zgodnie z dyktatem wyuczonej przez nich teorii. Większość z nich w istocie jedynie składa układanki, celując w odkrywaniu tego, co i tak już jest im znane. „Człowiek, który usiłuje rozwiązać problem zdefiniowany przez istniejącą wiedzę i technikę, nie ma szerszych horyzontów. Wie on, co chce osiągnąć, i w zgodzie z tym projektuje swoje narzędzia oraz kieruje swoimi myślami"[95].

Przez paradygmat należy zatem rozumieć całość, którą badamy i określamy na podstawie „użyć paradygmatycznych", a więc

paradygmatów w węższym znaczeniu tego słowa. Jednocześnie, ponieważ punktem wyjścia są tu wzorce i modele, nie dysponujemy od początku gotową, spójną i całościową teorią. W ten sposób zmiany wprowadzone przez Kuhna do jego pierwotnej koncepcji sprawiły, że w centrum uwagi badań nad paradygmatem znalazły się praktyki i schematy myślenia. Z tego też względu wyróżnione wcześniej momenty paradygmatu należy zmodyfikować o tyle, że pierwszy moment, związany z jego szerszym znaczeniem, zmienia się w paradygmat w węższym rozumieniu, a więc we wzorzec i model, na którego podstawie można w pewnej mierze określić ramy teorii.

Podstawowym elementem paradygmatu są prawa i teorie będące odpowiednikiem twardego rdzenia w programach badawczych Imre Lakatosa[96]. Ważną funkcję odgrywają również modele, które autor dzieli na heurystyczne i ontologiczne. Te ostatnie wyrażają przekonania o istnieniu określonych obiektów w rzeczywistości i jest to często element, który różni paradygmaty. Wartości naukowe są podstawą podejmowania decyzji o wyborze problemu oraz akceptacji bądź odrzuceniu rezultatów badań.

Nieco inaczej pojęcie paradygmatu objaśnia Leszek Nowak[97], który twierdzi, że są to „pewne koncepcje, które określają typ wyjaśnienia przyjętego w owej nauce w danym czasie za wzorcowy, albo inaczej – typ ostatecznych przesłanek wyjaśniających". Definicja ta podkreśla jego rolę w badaniach naukowych, zwłaszcza w wyjaśnianiu zdarzeń i procesów. W tym ujęciu paradygmatem jest teoria, „której tezy stanowią ostatnie – w danej nauce i czasie – ogniwa owego łańcucha eksplanacyjnego". Koncepcja Nowaka nie pozostaje w sprzeczności z podejściem Khuna[98], ponieważ również zakłada obecność teorii w paradygmacie. W związku z tym powstaje pytanie, która teoria pełni funkcję paradygmatyczną w wyjaśnianiu i prognozowaniu rozwoju społeczno-gospodarczego? Ostateczną przesłanką mogą być przekonania podzielane przez wspólnotę naukową obecne *implicite* w różnych teoriach[99].

Paradygmat bezpieczeństwa zawierający: podmiot bezpieczeństwa, przedmiot bezpieczeństwa, środowisko, w którym

bezpieczeństwo to jest zapewniane lub realizowane, oraz interakcje między wymienionymi składowymi, odnosi się do trzech domen, które nakładając się i przenikając, tworzą kontekst poznania oraz koncepcję tego poznania. Pierwszą domeną jest człowiek i otaczający go świat – świat działań człowieka, jego wytworów w świecie przyrody z ich wzajemnym przenikaniem. Drugą domenę stanowi otoczenie, w którym przebywa – społeczne i przyrodnicze. Trzecia domena natomiast to świat idei, dzięki którym ów człowiek rozpoznaje się w otaczającej go rzeczywistości (idee i budowane na ich podstawie ideologie można wyróżnić ze względu na ich specyfikę i właściwości, które określają działania człowieka, społeczności, społeczeństw, narodów)[100].

Biorąc to za punkt wyjścia, można wyróżnić charakterystyczne właściwości paradygmatu bezpieczeństwa wynikające z filozofii nauki i determinujące jednocześnie jego pojmowanie:

- bezpieczeństwo podmiotu jest identyfikowane statycznie jako swoisty „kadr", w którym została uchwycona rzeczywistość społeczna, i ten sposób ujęcia jest najbardziej oczywisty, gdyż obserwacja pozwala na określenie swoistych właściwości otaczającego nas świata;
- bezpieczeństwo jest pojmowane jako dynamiczny proces społeczny, w którym podmioty dążą do doskonalenia mechanizmów mających zapewnić im bezpieczeństwo[101];
- bezpieczeństwo podmiotu jest wyrażane w ujęciu pozytywnym – rozumianym jako cel o charakterze pozytywnym, tj. związanym z budowaniem, konstruktywną zmianą rzeczywistości, w której ma być zapewnione bezpieczeństwo, i negatywnym – rozumianym jako cel o charakterze negatywnym, związanym z brakiem (eliminacją) zagrożeń dla przeżycia, przetrwania[102].

Kategoria paradygmatu bezpieczeństwa obejmuje adekwatność konceptualizacji istoty tego zjawiska opierającej się na dostępnym stanie wiedzy. Według Andrzeja Urbanka należy go rozpatrywać w czterech zasadniczych wymiarach: ontologicznym (ukazanie, jakiego

rodzaju bytem, substancją jest bezpieczeństwo), epistemologicznym (granice i możliwości poznania oraz charakter generowanej wiedzy o tym zjawisku), metodologicznym (jak należy je badać – założenia teoretyczno-metodologiczne, strategie, procedury, metody, techniki, narzędzia), aksjologicznym (czemu służy bezpieczeństwo, co daje zgłębianie jego istoty)[103], ale także – jak zauważa Marian Cieślarczyk – w wymiarze piątym prakseologicznym (jak efektywnie je kształtować)[104]. Rozwój teorii bezpieczeństwa wymaga przede wszystkim doskonalenia prowadzonych badań, a w ślad za tym sposobu deskrypcji i konceptualizacji.

Paradygmat realistyczny koncentruje się na bezpieczeństwie państwa, gdyż realiści uważają, że to państwa są jedynymi lub głównymi uczestnikami stosunków międzynarodowych. Paradygmat ten akcentuje też czynnik militarny i zwraca uwagę na brak zagrożeń militarnych oraz działania nakierowane na ich eliminowanie.

Z kolei realizm polityczny wywodzi się z tradycji hobbezjańskiej i opiera się na założeniu, że bezpieczeństwo jest naczelnym celem polityki państw, które są podstawowymi aktorami stosunków międzynarodowych. Bezpieczeństwo jest kształtowane przez przemoc stosowaną przez państwa w anarchicznym systemie międzynarodowym. Teoria ta preferuje tradycyjne, siłowe, zmilitaryzowane pojmowanie bezpieczeństwa, a koncentruje się na badaniu instrumentów potęgi i siły w polityce państw.

Paradygmat neorealistyczny tzw. realizmu strukturalnego kładzie nacisk na redystrybucję potęgi i siły w systemie międzynarodowym, lekceważy natomiast kwestie moralne i uczestników pozapaństwowych[105].

Kluczowe znaczenie w badaniach prowadzonych z perspektywy realistycznej ma sformułowany kilkadziesiąt lat temu tzw. dylemat bezpieczeństwa oparty na schemacie „gry o sumie zerowej". Wskazuje on, że wzmocnienie bezpieczeństwa jednego państwa oznacza automatycznie osłabienie stanu bezpieczeństwa jego przeciwnika czy rywala. Realiści koncentrują się więc na ochronie państwa przed zagrożeniami zewnętrznymi, zapewniającej

równocześnie dobrobyt będącego wewnątrz społeczeństwa. Nie interesuje ich ustrój państwa i sprawy wewnętrzne.

Kolejnym szeroko rozpowszechnionym paradygmatem jest liberalizm, nazywany także idealizmem. Czerpie on inspiracje z myśli Johna Stuarta Milla, Jeremy'ego Benthama, liberalizmu ekonomicznego Adama Smitha i Davida Ricardo oraz idealizmu Immanuela Kanta. Liberalizm zakłada, że bezpieczeństwo jest celem różnych uczestników życia społecznego, w tym międzynarodowego, a najlepszą metodą jego zapewniania jest pokojowa współpraca, co akcentuje zwłaszcza tzw. nurt wilsonowski[106]. Jego przedstawiciele, od Davida Mitrany'ego po Johna Burtona, Richarda Ullmana, Michaela Doyle'a, Roberta Keohane'a i Josepha Nye'a oraz Andrew Moravcsika, wskazują, że pokój można zapewnić w przyszłości nie przez dążenie do równowagi sił, ale zabezpieczając potrzeby wszystkich narodów i demokratyzację życia międzynarodowego oraz wzmacniając instytucje międzynarodowe[107].

Nowy liberalizm zainicjowany przez Andrew Moravcsika[108] opiera się na trzech założeniach odpowiadających poszczególnym poziomom analizy, którymi są: poziom jednostki, poziom państwa i poziom systemu międzynarodowego. Powinnością państwa jest jedynie reprezentowanie interesów aktorów wewnętrznych za granicą, na arenie międzynarodowej. Od tego jest uzależniona strategia międzynarodowa państwa. Na preferencje państwa nie mają wpływu uwarunkowania międzynarodowe. Moravcsik twierdzi[109], że interesy państw nie są ani jednoznacznie sprzeczne (jak utrzymują realiści) ani zbieżne (co zakładają neoliberalni instytucjonaliści), lecz ograniczone przez interesy innych państw ze względu na współzależność występującą w stosunkach międzynarodowych.

Podejście liberalne odrzuca „dylemat bezpieczeństwa" i wskazuje, że współzależność interesów bezpieczeństwa państw może mieć także charakter pozytywny, co najpełniej się uwidacznia w systemie bezpieczeństwa międzynarodowego. Działalność na jego rzecz jest więc sprawdzonym sposobem umacniania bezpieczeństwa narodowego pojedynczych państw. Jego zaletą jest to, że państwa,

dążąc do umacniania swojego bezpieczeństwa, nie czynią tego kosztem interesów innych krajów, traktując je po partnersku, a nie jak przeciwników[110].

Według Paula D. Williamsa[111] przestrzeń badania bezpieczeństwa określają cztery pytania: czym jest bezpieczeństwo, o czyje bezpieczeństwo chodzi, co zalicza się do zagadnień bezpieczeństwa, jak można zapewnić bezpieczeństwo. Pytania te można traktować jako kolejne etapy, filary refleksji nad fenomenem bezpieczeństwa, opierającej się nie tylko na stanie aktualnej wiedzy, lecz także na wynikach dokonywanych penetracji empirycznych. Wprawdzie pierwsze z pytań jest bezpośrednio związane z konceptualizacją dokonaną w kolejnym podrozdziale, ale wróćmy do tego wątku, ukazując dokonujący się tu, interesujący i obiecujący nie tylko poznawczo, lecz także praktycznie (pragmatycznie) proces. W diachronicznie ujmowanym toku definiowania pojęcia „bezpieczeństwo" nietrudno zauważyć istotną ewolucję[112].

Początkowo w naukach społecznych dominowały definicje i koncepcje politologicznej proweniencji zawężające *de facto* istotę bezpieczeństwa do dwóch obszarów – państwa i stosunków międzynarodowych. W naukowym dyskursie dominujący był państwocentryczny paradygmat konceptualizacji zjawiska bezpieczeństwa. A przecież prymarnym odniesieniem ludzkiego bezpieczeństwa jest człowiek – jednostka, a nie państwo. Zanim powstało państwo, w obrębie pierwotnych kultur były konstruowane mechanizmy bezpieczeństwa człowieka, które następnie podlegały ewolucji kulturowej[113]. Przeważająca do niedawna narracja istoty bezpieczeństwa, zdominowana wymiarem *makro* – analizą na poziomie międzynarodowym bądź narodowym (państwowym) – wymagała więc niezbędnego dopełnienia naukową refleksją odnoszącą się do niższych poziomów ludzkich zbiorowości.

Perspektywa *mikro* (np. antropologiczna czy mikrosocjologiczna)[114], dotychczas wręcz niezauważalna, pozwala w inny sposób spojrzeć na problemy bezpieczeństwa: równoważyć wszystkie poziomy (z państwowym włącznie), a ponadto uwypuklić mechanizmy jego kształtowania i zarazem stymulować doskonalenie

tego procesu. Perspektywa ta może wnieść równocześnie ożywczy powiew do dyskusji na ten temat. I tak powstającą właśnie antropologię bezpieczeństwa można traktować nie tylko jako nową perspektywę poznawczą, lecz także jako nową możliwość integrowania problematyki bezpieczeństwa, swoistą – choć nie jedyną – płaszczyznę łączenia podstawowych wątków kreacji bezpiecznego życia, funkcjonowania i rozwoju człowieka oraz ludzkich zbiorowości. W takich okolicznościach „koncepcja bezpieczeństwa – zauważa znamiennie Stanisław Sulowski – przeszła ewolucję od pojęcia bezpieczeństwa wyjaśnianego przez państwo do bezpieczeństwa przedstawianego bez odwołania się do wszechpotężnej instytucji państwa”[115]. Nowe odsłony bezpieczeństwa, w nowych burzliwych czasach wymagają innych instrumentów i znacznie szerszej, bardziej wielostronnej i wnikliwej refleksji. W tym kierunku zmierzają więc tendencje klarujące się w zasadniczym nurcie rozwoju nauk o bezpieczeństwie.

W okresie tzw. dywidendy nauki wojskowe przesuwają swój akcent na zagadnienie pokoju, rozwijając przede wszystkim teorię bezpieczeństwa narodowego. Następnie, w procesie poszerzania tematyki bezpieczeństwa, różne dyscypliny powoli zaczęły rozwijać teorie podstawowych kategorii bezpieczeństwa przedmiotowego, a zarazem następowało obniżenie pułapu zainteresowania – na struktury społeczne niższych szczebli, aż po jednostkę[116]. Ta właśnie tendencja – poszerzania i pogłębiania bezpieczeństwa – doprowadziła do wykształcenia się nauk o bezpieczeństwie oraz nauk o obronności.

Nauki o bezpieczeństwie łączą nie tylko wojskowe teorie bezpieczeństwa, lecz także zróżnicowane i oryginalne wątki bezpieczeństwa rozwijane w kontekstach działania innych instytucji bezpieczeństwa, takich jak służby specjalne, policja, służby graniczne, straż pożarna itp. Nauki o obronności kontynuują głównie wątki rozwijane dotychczas przez klasyczne nauki wojskowe. Istotną słabością dotychczasowego teoretycznego dyskursu w obszarze istoty bezpieczeństwa jest wyraźny niedobór uniwersalizmu – powszechna maniera definiowania realnych desygnatów (zwłaszcza

np. bezpieczeństwa państwa, bezpieczeństwa narodowego i bezpieczeństwa międzynarodowego), a nie bezpieczeństwa jako fenomenu, ze zminimalizowanym odniesieniem do ściśle określonego podmiotu – jednostkowego lub zbiorowego[117]. Wprawdzie bezpieczeństwo nie stanowi bytu *sui generis* (i zawsze jest stanem określonego podmiotu, obiektu), ale jako fenomen ludzkiej egzystencji (przyjmującej zróżnicowane formy) musi mieć konstrukt uniwersalny, tak jak w przypadku szczęścia, miłości, twórczości czy walki.

Jeżeli mamy do czynienia z multigatunkowym podmiotem zjawiska bezpieczeństwa, to można oczywiście definiować bezpieczeństwo każdego z nich. Tylko co to wnosi do teorii? Takie podejście jest właściwe na poziomie analitycznym, nakierowanym na praktykę, lecz mniej – na poziomie teoretycznym. Tak jak w określonych sytuacjach (głównie na potrzeby praktyki) niezbędne jest definiowanie konkretnych desygnatów bezpieczeństwa, tak występuje jednocześnie potrzeba uniwersalistycznej analizy, poszukującej owego konstruktu[118]. Ze względu na swój egzystencjalny charakter bezpieczeństwo należy bowiem do podstawowych wartości uniwersalnych. Takich podejść i analiz – przy ogólnej nadpodaży publikacji nadmiernie ogólnikowych (co często wynika z ich odtwórczego charakteru) czy też zreifikowanych – jest stanowczo za mało. Zasadniczy instrument doskonalenia paradygmatu bezpieczeństwa tkwi w aktywności badawczej. Tutaj największe trudności sprawia charakter „żywych" zjawisk bezpieczeństwa.

Inną kwestią jest swoista incydentalność pewnej klasy samoistnych zjawisk naruszających bezpieczeństwo, a trudno zgłębić jego istotę, nie odnosząc się do sfery realnych, czynnych zagrożeń[119]. Występują one wprawdzie na całym globie, ale spontanicznie, nieprzewidywalnie i nieobliczalnie, w wyniku czego badaczowi niejednokrotnie trudno „zdążyć" na ich bezpośrednią obserwację. Ogólnie dostępne zjawiska przemocy domowej, ubóstwa, bezrobocia czy odrzucenia społecznego nie mogą zastąpić realiów trzęsienia ziemi, katastrofy morskiej czy lotniczej, a także zamachu

terrorystycznego czy też klasycznego napadu na bank i wynikających stąd wartości poznawczych.

Strategią zaradczą – w kontekście wymienionych osobliwości – staje się stosowanie metody analizy doniesień medialnych. Można założyć, że w obecnych czasach media są „oczami społeczeństwa", pojawiają się wszędzie i są w gotowości do rejestrowania zjawisk bezpieczeństwa oraz ich wstępnej analizy i komunikacji społecznej oraz publikacji. Zatem dokonując systematycznej i gruntownej lustracji tych doniesień, można pozyskiwać cenny badawczo materiał. Metoda analizy doniesień medialnych w dużym zakresie korzysta z techniki analizy treści, ale nie jest jej tożsama. O ile praca nad treścią pozostaje niejako w obu przypadkach analogiczna, o tyle analiza doniesień medialnych nadbudowuje całą technologię wyszukiwania źródeł treści adekwatnych do przedmiotu badań, ich filtracji, co w czasach cywilizacji informacyjnej (wszechogarniającego Internetu) staje się nowym obszarem aktywności badawczej[120].

Inną kwestią jest problem wiarygodności danych medialnych. Występuje tu potrzeba ich ścisłej weryfikacji jako istotny element procedury badawczej. Wyjściem z sytuacji jest postulat triangulacji pozyskiwania danych (stosowanych metod i poddawanych analizom danych), czyli pozyskiwanie (uwzględnianie) danych z różnych źródeł oraz ich interpretacja z różnych punktów odniesienia. Aby zyskać pewność, należy konfrontować pozyskane dane z różnych źródeł. Można je również weryfikować *post factum* w miejscu zdarzeń. Należy również uwzględnić zagrożenie związane z selektywnością pozyskiwanych danych. Selektywność zarówno danych prezentowanych przez media, jak i dostępności badacza do takich danych, a także dokonywanej przez niego kwerendy sprawiają, że formułowane wnioski, teorie mogą posiadać pewne niedostatki, przekłamania, a nawet jawić się jako nieadekwatne do rekonstruowanej rzeczywistości. Jednak nawet taki stan rzeczy może mieć swoje dobre strony. Jak pisał Ralf Dahrendorf: „fałszywa teoria – taka, której fałszywości można dowieść – jest lepsza niż żadna,

ponieważ odrzucenie złej teorii jest z reguły kamieniem milowym na drodze ku lepszej”[121].

Trzeba też wspomnieć o krytycznej analizie dyskursu, która pozwala lepiej wykorzystać potencjał naukowy tkwiący w przekazach medialnych, a zasadniczo w tekstach pisanych. Polega ona ogólnie na zrekonstruowaniu dyskursu na temat konkretnych „aktów” bezpieczeństwa – wskazaniu mechanizmów dyskursywnych, schematów interpretacyjnych oraz rekonstrukcji głównych mechanizmów bezpieczeństwa wyłaniających się z analizowanych tekstów. Podejmując analizę dyskursu, zwraca się uwagę na trzy zasadnicze elementy: kontekst dyskursu, typy dyskursu i ewolucję, dynamikę dyskursu. Immanentnym jej elementem jest również procedura zbierania, analizy i interpretacji tekstów. Badanie bezpieczeństwa nie może nie uwzględniać założeń metodologii systemowej. Bezpieczeństwo stanowi przecież ważną charakterystykę antroposystemu, który Stanisław Zięba określa jako „system interaktywny między dwiema całościami ukonstytuowanymi przez socjosystem i ekosystem w danej przestrzeni geograficznej i podlegający ewolucji w czasie”[122]. Studia antroposystemu opierają się na analizie strukturalnej i funkcjonalnej systemów kompleksowych, gdzie nakładają się i wzajemnie oddziałują procesy (dynamiki) naturalne oraz społeczne[123]. Przedmiotem badań problemów bezpieczeństwa powinien być kompleks zmiennych sytuujących się w triadzie: socjosystem, antroposystem i ekosystem (z modułem ekokulturowym włącznie).

Według Piotra Sienkiewicza[124] procedura systemowa, w przypadku badań nad bezpieczeństwem, może przyjąć formę opierającą się na następujących podstawach:

- ujmowania zjawiska zagrożeń i bezpieczeństwa w kategoriach systemu, czyli podsystemów w określony sposób zależnych od siebie oraz od własności systemowych;
- analizy ogółu warunków zewnętrznych, czyli relacji z bliższym i dalszym otoczeniem systemowym, ze szczególnym

uwzględnieniem zagrożeń i zakłóceń mających destrukcyjny wpływ na działanie systemu;
- prognozowania przyczyn zagrożeń i ich skutków wewnętrznych przekształceń systemu, jego zdolności samosterowania i samoorganizacji, koordynacji i adaptacji do zmian w otoczeniu;
- analizy funkcjonowania systemu w aspekcie podatności (odporności) na zagrożenia zgodnie z przyjętymi kryteriami efektywności;
- ewaluacji i analizy decyzyjnej: dążenia do formułowania rozwoju bezpieczeństwa systemu w kategoriach (wielokryterialnej, wieloatrybutowej) optymalizacji strategii.

W konkluzji wyraźnie rysuje się teza o wieloparadygmatycznym charakterze badań bezpieczeństwa. Już nauki o bezpieczeństwie mają taki charakter[125]. Jeśli dodamy do tego rozległe obszary wiedzy o człowieku, społeczeństwie i kulturze, pojawia się nad wyraz złożona, wielogatunkowa konstrukcja metodologiczna, obejmująca mnogość podejść teoretyczno-metodologicznych, orientacji i paradygmatów badawczych, metod, technik z całym zapleczem interdyscyplinarności[126]. W ślad za aktywnością badawczo-empiryczną paradygmat bezpieczeństwa konkretyzuje się także na płaszczyźnie jego teoretyzacji – dzięki aktywności rzeszy wybitnych umysłów, materializowanej w ważnych publikacjach.

Poszukując uniwersalnego paradygmatu bezpieczeństwa, Jarosław Gryz[127] wskazuje, że decydują o nim charakter założeń, przyjęta wielokryterialność oraz kontekst bezpieczeństwa. Trzecią płaszczyzną doskonalenia paradygmatu bezpieczeństwa jest zatem działalność praktyczna na rzecz jego kształtowania. Należy tu wskazać przede wszystkim na aktywność przygotowującą do takiego działania. Jest nią bez wątpienia edukacja dla bezpieczeństwa[128]. W perspektywie tej dyscypliny bezpieczeństwo jest więc problemem edukacyjnym.

2.2
EUROPEJSKA STRATEGIA BEZPIECZEŃSTWA JAKO INSTRUMENT POLITYKI CYBERBEZPIECZEŃSTWA UNII EUROPEJSKIEJ

Rozważania na temat strategii bezpieczeństwa należy rozpocząć od zdefiniowania pojęcia, aby przejść do innych kwestii w tym podrozdziale. Trzeba najpierw odpowiedzieć na pytanie, czym jest strategia. Strategia wywodzi się od greckiego słowa *strategikos* – strategia, czyli dowodzenie wojskiem, inaczej wojskowy plan przygotowania i prowadzenia walk[129].

Strategia jako główny dział sztuki wojennej obejmuje teorię i praktykę przygotowania oraz prowadzenia wojny, jej poszczególnych kampanii i najważniejszych operacji[130]. Czym więc jest? Jeśli rozpatrywać to pojęcie w aspekcie praktycznym, to strategia jest sposobem (metodą) działania, jednak z pewnością sposobem specyficznym, odróżniającym go od innych. Należy zatem wykazać, na czym polega ta specyfika i jak często występuje. Według wszelkich kryteriów strategia jest nauką[131]. Istotną cechą strategii bezpieczeństwa jest wysoki poziom uogólnienia w myśleniu i działaniu. Upraszczając, możemy przyjąć, że strateg, mając określony cel i wydzielone siły oraz środki, musi umieć wytyczyć konkretny, racjonalny sposób postępowania (scenariusz) do osiągnięcia tego celu, mimo że szczegóły wykonania zadania mogą temu sprzyjać lub nie. Związane z tym szczegóły nie mogą jednak przesłonić przyjętego sposobu działania zmierzającego do osiągnięcia głównego celu. Należy dodać, że umiejętność uogólnionego myślenia i działania w wymiarze strategicznym może być umiejętnością wrodzoną lub nabytą. Niektórzy zdobywają ją w praktycznym działaniu, w różnych złożonych sytuacjach.

Odpowiadając w dalszej części rozważań na pytanie, czym jest strategia bezpieczeństwa, należy stwierdzić, że jest także nauką, specjalnością naukową wchodzącą w skład nauk społecznych. Aby lepiej zrozumieć istotę strategii bezpieczeństwa, trzeba by

odtworzyć ponownie treść definicji niektórych autorów – klasyków, na podstawie dostępnej literatury.

W klasycznym rozumieniu pojęcie strategii dotyczyło spraw wojny i wojska rozpatrywanych z pozycji naczelnego dowódcy odpowiedzialnego za przygotowanie armii i prowadzenie wojny. Tak było przez wiele wieków. Obecnie już tylko nieliczni dowódcy decydują o wojnach czy o wielkości armii, ponieważ na ogół czynią to politycy. Oni bowiem decydują o celu wojny, siłach zbrojnych, sojuszach i innych czynnikach, które wynikają z polityki. Nie należy ignorować roli wielkich dowódców, ponieważ oni też mają swój udział w kształtowaniu strategii osiągnięcia celów politycznych, ale nie jest to element decydujący. Przebieg wojny coraz częściej zależy od wielu parametrów pozamilitarnych, takich jak czynniki: polityczne, ekonomiczne, społeczne, ekologiczne, psychologiczne, kulturowe, a nawet religijne. To powoduje, że naczelny dowódca musi je uwzględniać podczas planowania operacji militarnych.

W celu przeprowadzenia kompleksowej analizy i oceny sytuacji dowódca przed podjęciem decyzji korzysta z pomocy merytorycznej specjalistów danej dziedziny wiedzy. Nie bez znaczenia pozostają w rozwoju strategii słowa Carla von Clausewitza, którego maksyma brzmi: „Wojna jest nie tylko czynem politycznym, lecz prawdziwym narzędziem polityki, dalszym ciągiem stosunków politycznych, przeprowadzeniem ich innymi środkami”[132]. W tym znaczeniu obarcza on odpowiedzialnością za wojnę i jej skutki politykę, definiując wyraźnie wojnę jako instrument polityki, jako akt siły dla zmuszenia przeciwnika do spełnienia naszej woli. Dlatego wojna staje się środkiem osiągnięcia celu politycznego. Współcześnie sentencja Clausewitza, dotycząca polityki, jest wciąż aktualna[133].

Według Carla von Clausewitza strategia „jest nauką o użyciu bitew dla celów wojny”[134]. Należy przypuszczać, że autor arbitralnie i prospektywnie uznał bez dodatkowych wyjaśnień, że strategia jest nauką. Ten wybitny strateg postąpił tak pod wpływem różnych uwarunkowań wewnętrznych i zagrożeń zewnętrznych w dobie XIX w.

Z kolei Basil H. Liddell Hart[135] – angielski teoretyk strategii, uczestnik I wojny światowej – wyróżnia strategię i wielką strategię. Uważa, że wielka strategia to sztuka rozdziału i użycia środków wojennych, rodzaj polityki prowadzącej do osiągnięcia rzeczywistych celów politycznych. Czysta strategia, strategia militarna albo tylko strategia natomiast prowadzą do osiągnięcia celów militarnych. Liddell Hart widział zasadniczą różnicę między polityką a strategią. Według niego polityka determinuje priorytety działania, które z kolei określają cele strategiczne. Priorytety polityczne nie dotyczą tylko wojny, lecz również celów wynikających z interesów narodowych. Był strategiem oryginalnym, uważał, że użycie środków wojennych niekoniecznie miało oznaczać ich wykorzystanie w walce zbrojnej. Według niego, jeśli dochodzi do bitwy, to w sposób pośredni powinno doprowadzać do sytuacji, w której zwycięstwo jest pewne.

Powszechnie uznawany klasyk, Francuz André Beaufre uważa, że strategia to „sztuka dialektyki woli, stosująca siłę dla rozwiązywania konfliktu”[136]. Definicja Beaufre’a[137], mimo że nie odbiega od pojęcia Clausewitza, ma jednak cechę zasadniczą – jest oryginalna. Zawiera wiele abstrakcji, chociaż odpowiada każdej konfliktowej, złożonej sytuacji. To oznacza, że ma charakter współczesny w każdym obszarze, dlatego jej uniwersalność jest niepodważalna, przynajmniej na obecnym etapie rozwoju nauki o strategii. Zdaniem Beaufre istota strategii tkwi w abstrakcyjnej grze, która wynika z przeciwieństwa woli dwóch stron. Jest to sztuka pozwalająca, niezależnie od wielkiej techniki, opanować problemy wynikające z każdego pojedynku, aby właśnie dzięki temu móc stosować technikę w sposób najbardziej skuteczny. Bezsporną zasługą Beaufre stało się opracowanie teorii odstraszania, która ma szczególne znaczenie w dobie broni jądrowej. Jego prace znalazły miejsce na półkach bibliotecznych niemal wszystkich uniwersytetów i akademii wojskowych.

W Polsce było wielu teoretyków zajmujących się strategią. Do znanych autorów strategów w okresie międzywojennym możemy zaliczyć: Mossora, Abżółtowskiego, Rolę-Arciszewskiego, Jureckiego,

Romeykę[138]. W swoich pracach prezentowali poglądy niekiedy bardzo zbliżone do myślicieli światowych w zakresie strategii. Teoretykiem z tej dziedziny o szczególnie interesującym dorobku naukowym był gen. Władysław Sikorski. Jego książka *Przyszła wojna* z 1934 r. została przetłumaczona na kilka języków. To on przewidział, że w II wojnie światowej zwycięzcą będzie Związek Sowiecki. A przecież do wojny nie były przygotowane ani Związek Sowiecki, ani Francja, ani Wielka Brytania[139].

Do polskich znawców problemów strategii należy również gen. Franciszek Skibiński, który następująco sformułował definicję strategii: „Strategią nazywamy sposób postępowania w przygotowaniu i prowadzeniu danej konkretnej wojny, kampanii lub bitwy, obrany i stosowany przez najwyższe ogniwa władzy państwowej, naczelne dowództwo sił zbrojnych lub naczelne dowództwo danego konkretnego teatru działań wojennych”[140]. Strategia jest więc najwyższym działem teorii i praktyki sztuki wojennej, a więc przymiotnik „strategiczny” odnosi się do zagadnień związanych ze sprawą prowadzenia wojny, kampanii i bitwy przez wymienione ogniwa władzy państwowej i wojskowej w fazie zarówno studiów, przygotowania, jak i wypełnienia. Do tej definicji można mieć zastrzeżenie natury merytorycznej, jeśli bowiem strategia jest teorią i praktyką, a praktyka wchodzi w skład sztuki wojennej, to na pewno nie zawiera ona teorii strategii. W zasadzie rozgraniczenie nie jest tu konieczne, ponieważ czym innym jest teoria, a czym innym praktyka oraz sztuka.

W istocie narzędziem realizacji polityki w zakresie bezpieczeństwa jest polistrategia. Jej obszar jest znaczny, gdyż obejmuje wszystkie elementy struktury bezpieczeństwa narodowego wynikające z celów wyznaczanych przez politykę. W pewnym uproszczeniu można przyjąć, że cele polityki bezpieczeństwa stają się jakby celami polistrategii. W przypadku polistrategii bezpieczeństwa narodowego, która ma służyć określonym wyzwaniom i zapobieganiu zagrożeniom, jej działania mogą i powinny być wyprzedzające. Każdy cel powinien być precyzyjnie i jednoznacznie określony z wyznaczeniem terminu i przestrzeni jego realizacji[141]. Możemy już

teraz bez większego błędu przyznać, że polistrategia bezpieczeństwa narodowego obejmuje wszystkie dziewięć kategorii bezpieczeństwa wewnętrznego państwa, tj. polityczne, ekonomiczne, militarne, publiczne, ekologiczne, informacyjne, społeczne, kulturowe i religijne.

Polistrategia bezpieczeństwa zewnętrznego natomiast obejmuje systemy polityczne państw, globalizację, regionalizację i instytucjonalizację oraz politykę zagraniczną państw. Celem polityki jest konsekwentne zapobieganie zagrożeniom i tworzenie jak najkorzystniejszego otoczenia państwa oraz umacnianie jego międzynarodowej pozycji, wizerunku i prestiżu. Należy tworzyć i rozwijać zdolności do osiągania narodowych celów strategicznych w dziedzinie bezpieczeństwa w bezpośrednim sąsiedztwie, w przestrzeni europejskiej, euroatlantyckiej i globalnej. Nie należy lekceważyć również uwarunkowań, które tworzą warunki umacniania powiązań oraz mechanizmów wspólnotowych i sojuszniczych[142].

Strategia bezpieczeństwa politycznego obejmuje obszar, który bezpośrednio wiąże się z przeciwdziałaniem zagrożeniom o treści politycznej wywodzącej się z systemu stosunków międzynarodowych. Działania wobec tych zagrożeń muszą być postrzegane w kontekście funkcjonowania państwa na arenie międzynarodowej w regionie (UE). Zagrożenia o charakterze politycznym zawsze dotyczą wartości najistotniejszych, najczęściej sięgających racji stanu, tj. suwerenności, integralności, tożsamości i rozwoju. Dlatego właśnie cele strategii bezpieczeństwa politycznego są ogólnikowe, długookresowe i najczęściej zbieżne z celami polityki zagranicznej państwa.

Obszarem (przestrzenią) bezpieczeństwa politycznego natomiast zawsze jest terytorium państw sąsiednich bądź państw regionu (sojuszu), w którym dany kraj się znajduje. Niekiedy ten obszar bezpieczeństwa, zwłaszcza w warunkach globalizacji, może się poszerzać o inne kontynenty w ramach funkcjonowania państwa w ONZ. Bezpieczeństwo polityczne może być realizowane wtedy w obszarach pozaeuropejskich, w dalszym otoczeniu. Dotyczy to przede wszystkim kryzysów polityczno-militarnych w odległych

regionach, które mogą oddziaływać na bezpieczeństwo polityczne konkretnego państwa. W takiej sytuacji powinno się zapobiegać im, m.in. przez włączenie się do wysiłków międzynarodowych w zakresie dyplomacji prewencyjnej[143]. Zasadniczą rolę odgrywają tu umiejętności osób odpowiedzialnych za formułowanie i prowadzenie polityki zagranicznej, a zwłaszcza tych jej problemów, które dotyczą bezpieczeństwa państwa[144].

Z kolei strategia bezpieczeństwa ekonomicznego ma nie mniejsze znaczenie niż bezpieczeństwo polityczne w systemie bezpieczeństwa narodowego. Można zaryzykować twierdzenie, że nie ma racjonalnej polityki państwa bez prężnej, zdrowej i efektywnej gospodarki, czyli ekonomii. W dobie toczących się procesów globalizacji i integracji kwestia ekonomizacji i bezpieczeństwa musi być nie tylko postrzegana, lecz także konsekwentnie urzeczywistniana. Strategia bezpieczeństwa ekonomicznego powinna uwzględniać przede wszystkim podstawowe wartości, tj. ochronę poziomu życia, rozwój gospodarczy i zdolność utrzymania bezpieczeństwa państwa[145]. Wynika to z faktu, że gospodarka tworzy materialną bazę państwa w jego zasadniczych obszarach bezpieczeństwa. W porównaniu do celów będących elementem innych strategii sektorowych cele strategii bezpieczeństwa ekonomicznego muszą się cechować większym realizmem polegającym na uwzględnieniu warunków i środków będących w dyspozycji państwa. Cele zbyt ambitne, pozbawione realizmu, mogą świadczyć jedynie o braku kompetencji i woluntaryzmie. W związku z nasilającymi się procesami globalizacji i integracji w skali regionów gospodarek różnych państw, o różnym poziomie rozwoju, przy określaniu celów strategii bezpieczeństwa ekonomicznego poszczególne kraje muszą uwzględniać globalny i regionalny kontekst, zwłaszcza autonomiczne i często ekspansywne dążenia ponadnarodowych koncernów i korporacji. Ponadto celem strategii bezpieczeństwa ekonomicznego powinny być działania na rzecz doskonalenia mechanizmów regulujących w gospodarce światowej, a zwłaszcza regulowania przepływów finansowych.

Strategia bezpieczeństwa militarnego zajmuje należne miejsce[146] w systemie bezpieczeństwa narodowego. Cele strategii militarnej

odnoszą się do systemu wartości danego państwa, czyli muszą wynikać z ogólnych celów polityki państwa w zakresie bezpieczeństwa militarnego. Koncepcja bezpieczeństwa militarnego jest zawarta w założeniach strategii obronnej państwa, która wyraźnie wskazuje gotowość do obrony terytorium, niepodległości i suwerenności danego państwa. Strategia bezpieczeństwa militarnego powinna cechować się realizmem i uwzględniać konflikty regionalne i lokalne, które występują w bliższym i dalszym otoczeniu państwa. Współcześnie pojmowane bezpieczeństwo militarne państwa to relacja, jaka zachodzi między państwem a środowiskiem międzynarodowym, w której uczestniczy czynnik militarny.

Duże znaczenie bezpieczeństwa publicznego wynika z zagrożenia w świecie, regionie i państwie, w jakim żyjemy. Poczucie bezpieczeństwa jest funkcją poczucia zagrożenia, a to ostatnie rośnie z każdym dniem. Stan poczucia zagrożenia negatywnie wpływa na rozwój cywilizacyjny jednostki i społeczności, gdyż oddziałuje na kształtowanie warunków życia podmiotu. Znaczenie bezpieczeństwa publicznego określa jego definicja: „Bezpieczeństwo publiczne to stan na obszarze państwa powstały w wyniku zorganizowanej i realizowanej obrony i ochrony osób oraz mienia przed zagrożeniami na lądzie, morzu i w powietrzu (kosmosie)”. Dla urzeczywistnienia tak sformułowanej definicji powstają systemy bezpieczeństwa publicznego w państwie wprowadzane ustawami. W każdym przypadku za bezpieczeństwo publiczne w państwie odpowiada właściwy (konstytucyjny) minister spraw wewnętrznych, a podstawowym organem wykonawczym jest policja. Strategia bezpieczeństwa ekologicznego charakteryzuje się tym, że bardzo często obejmuje obszary transgraniczne, a więc określoną część lub całość terytorium państwa powiększoną o przestrzeń zewnętrzną. Narastająca skala zjawiska ekologii nabiera cech globalnych.

Strategia bezpieczeństwa społecznego charakteryzuje się tym, że jej cele obejmują zwykle krótszy horyzont czasowy. W aspekcie przestrzennym odnosi się ona do sytuacji istniejącej w państwie. Podstawowym warunkiem rozwoju państwa we wszystkich jego obszarach jest natomiast pokój społeczny, tj. zaakceptowanie przez

społeczeństwo istniejącej struktury państwa demokratycznego i organów władzy publicznej. Społeczeństwo demokratyczne, w którym władza uległa decentralizacji, jest podstawowym czynnikiem mającym znaczący wpływ na oblicze[147] kraju, którego siła opiera się na walorach moralnych obywateli, ich skłonności do działań prospołecznych, a także uznaniu dobra wspólnego nad dążeniami indywidualnymi. Oznacza to społeczeństwo, któremu są obce różnego rodzaju przestępstwa, zwłaszcza gospodarcze. Istotą bezpieczeństwa społecznego, jako naczelnej wartości, jest życie nie tylko jednostki, lecz także grupy społecznej, całego społeczeństwa oraz grupy państw we współczesnym świecie. Dwa ważne wskaźniki, jakimi są gwarancja funkcjonowania danego podmiotu i pewność jego przetrwania, dają możliwość zarówno jego działania, jak i rozwoju. Z dotychczasowych rozważań wynika, że w narodzie, w którym państwo ustanowiło trwałe warunki bytu i rozwoju, zachodzą różne procesy wspierające to dobro lub jemu zagrażające. Państwo może mieć korzystny klimat społeczny do wypełniania swojej misji albo może być zagrożone z różnych przyczyn wewnętrznych lub zewnętrznych, a niekiedy jednych i drugich w tym samym czasie.

Po zakończeniu II wojny światowej ówczesne mocarstwa – Stany Zjednoczone Ameryki, Związek Sowiecki, Wielka Brytania, Chiny i Francja – zagwarantowały sobie stałe miejsce (stałego członka) w Radzie Bezpieczeństwa ONZ i prawo weta. Była to z ich strony odmowa przekazania części uprawnień wynikających z suwerenności na rzecz organizacji międzynarodowej, polityki bezpieczeństwa, pewnych form kontroli międzynarodowej, co uczyniły wszystkie państwa będące członkami ONZ[148]. Ideologiczna i ekonomiczna przepaść, jaka nastąpiła między mocarstwami, tj. Stanami Zjednoczonymi i Związkiem Sowieckim, kształtowała charakter zimnej wojny, wzmacniała dwubiegunowy układ międzynarodowy i stymulowała wzajemną rywalizację, doprowadzając do wyścigu zbrojeń na niespotykaną w dziejach ludzkości skalę. Stany Zjednoczone, wypełniając mesjanistyczną wizję Woodrowa Wilsona, czyli poszerzenia cywilizacji opartej na zasadach demokratycznych i stosowania etyki w polityce zagranicznej oraz stosunkach

międzynarodowych, czuły się obrońcą państw zagrożonych przez komunizm. W tym celu Waszyngton posługiwał się strategią powstrzymywania, sformułowaną w doktrynie opracowanej przez George'a Kennana. Podstawowe założenia tej strategii zaprezentował 12 marca 1947 r. prezydent USA Harry Truman[149].

Dominujący po zakończeniu II wojny światowej realizm dość szybko zaczął ulegać mutacjom, głównie pod wpływem zmian w polityce i gospodarce światowej oraz ewolucji międzynarodowego środowiska bezpieczeństwa. Pojawia się neorealizm nazywany także strukturalnym realizmem, odradza się też idealizm w formie neoliberalizmu w dwóch odmianach: pluralizmu i strukturalizmu. Neorealiści podkreślają znaczenie państw w stosunkach międzynarodowych, a także siły i bezpieczeństwa militarnego. Neoliberaliści nadal uznają za istotne idee współpracy międzynarodowej, skuteczny multilateralizm, doceniając wagę siły militarnej, choć nie jako *ultimo ratio*[150].

Pozimnowojenna sytuacja ukazywała, że Stany Zjednoczone są jedynym mocarstwem uniwersalnym, dominującym nad państwami Europy militarnie i gospodarczo. Po upadku komunizmu zwycięska ideologia umacniała amerykańską pewność i przekonanie o wypełnianiu światowej misji demokratyzacji, do czego przekonywał swojego czasu Wilson. W związku z tym wiodącymi elementami były obrona interesów nawet na drodze wojny, dbanie o równowagę sił na świecie, aby potencjalni nawet wrogowie nie umacniali się nadmiernie, zagrażając bezpieczeństwu państwa[151].

Radykalna i gwałtowna zmiana w stosunkach międzynarodowych nastąpiła w 1991 r. Koniec zimnej wojny, rozpad Związku Sowieckiego i doświadczenia lat 90. XX w. w obszarze stosunków międzynarodowych dokonały transformacji pojęcia i filozofii mocarstwowości oraz form jego przejawiania. Nastąpiła różnorodność zachowań, od tradycyjnego egoizmu mocarstwowego, braku zaangażowania z różnych przyczyn, aż po solidarność. Słabość organizacji międzynarodowych dbających o bezpieczeństwo dała się zauważyć podczas konfliktów militarnych, zbiorowych operacji stabilizacyjnych i pokojowych prowadzonych pod egidą mocarstw.

Doprowadziło to do większej swobody ich działań i próby wypełniania luki w stosunkach międzynarodowych. Jednocześnie nastąpił spadek napięcia ze względu na osłabienie wpływu systemu równowagi strachu na środowisko międzynarodowe[152].

Dla większości teoretyków kres zimnej wojny i upadek świata dwubiegunowego to cezura otwierająca nową kartę w sprawach bezpieczeństwa i w badaniach nad nim. Idealiści mogli więc z większym przekonaniem prezentować swoją optymistyczną wizję, realiści zaś twierdzili, że niewiele to zmieniło, ponieważ mocarstwa nadal dążyły do osiągania swoich celów za pomocą siły. Jedyne co ich zdaniem się zmieniło, to pojawienie się większej grupy aktorów niepaństwowych, choć nadal to głównie państwa decydowały o kształcie ładu i stosunków międzynarodowych[153].

Należy zauważyć, że współczesne pojmowanie realizmu i liberalizmu nie jest jednoznaczne. W konfrontacji ze światem występuje wiele sprzeczności i napięć wewnętrznych w obu teoriach, co utrudnia jasne scharakteryzowanie sposobu działania przedstawicieli posługujących się tymi koncepcjami. Pojawia się również wiele odmian i typów wewnątrz nurtów, ale w kwestiach zasadniczych istnieje między nimi daleko idący konsensus pozwalający na wyodrębnienie zasadniczych różnic i istoty postrzegania kwestii bezpieczeństwa[154].

W rzeczywistości międzynarodowej brakuje czynnika, który określałby reguły wzajemnego zachowania się państw, zapobiegał konfliktom między nimi i bronił przed napaścią. Założenia charakterystyczne dla realistów w gruncie rzeczy sprowadzają się do wąskiego rozumienia bezpieczeństwa opartego na atrybutach siły militarnej i poszukiwaniu równowagi sił w mającej cechy anarchiczne w sferze stosunków międzynarodowych[155]. Realizm polityczny natomiast, unikający konfrontacji ideologicznych i budujący pokojowe stosunki międzynarodowe oparte na równowadze sił, właściwym rozumieniu interesu narodowego i polityce powstrzymania (*containment*), okazał się skuteczny w kierowaniu polityką amerykańską w okresie zimnej wojny.

Koniec zimnej wojny i świata bipolarnego spowodował kryzys w myśleniu realistycznym, skoncentrowanym prawie wyłącznie na roli państw i potędze militarnej, oraz wzrost zainteresowania liberalizmem[156]. Orientacja ta bowiem traktuje bezpieczeństwo w szerokim – również pozytywnym – sensie, uwzględniając także jego pozamilitarne aspekty, i upatruje idealny system bezpieczeństwa międzynarodowego w modelu bezpieczeństwa zbiorowego. To za sprawą liberałów po I wojnie światowej sformułowano program „przebudowy" stosunków międzynarodowych i kreowania ładu międzynarodowego na innych zasadach niż tych proponowanych przez realistów. Mimo że obecnie liberałom daleko do utopijnych idei wilsonowskiego idealizmu okresu międzywojennego, dążą oni w stosunkach międzynarodowych do zastąpienia siły prawem, systemem porozumień i organizacji międzynarodowych. W świecie realistów współpraca międzynarodowa jest trudna, gdyż istnieje nieprzezwyciężalna rozbieżność interesów i naturalna konkurencja między państwami. Nie chodzi tu o rzeczywistą wojnę, ale stan, w którym wojna pozostaje w centrum uwagi – jej przygotowanie, kalkulacje bilansu sił skłaniające do agresywnych zachowań lub moderujące konflikt. Liberalna wrogość do wojny powodowała też wrogość do autorytaryzmu, bo według liberałów (poczynając od Kanta) powodem wszelkich konfliktów była władza autorytarna. Odpowiedzią liberałów na wojnę była wiara w idee demokracji.

W trakcie trzeciej debaty interparadygmatycznej w teorii stosunków międzynarodowych w latach 90. XX w. zrodził się konstruktywizm, który obok teorii krytycznej i postmodernizmu opiera się na założeniu, że w zasadzie nie istnieje obiektywna rzeczywistość społeczna jako taka. Ona i poszczególne jej segmenty są konstruktem społecznym, produktem życia społecznego, efektem jego wielokrotnej reinterpretacji i przynależą do tradycji badaczy[157].

Z tego wynika, że stosunki międzynarodowe czy bezpieczeństwo międzynarodowe nie istnieją samodzielnie, lecz jedynie jako intersubiektywna świadomość między ludźmi. Kluczowym założeniem konstruktywizmu jest to, że istniejący obiektywnie świat

materialny jest spowity siecią znaczeń i praktyk rozpoznawanych oraz podzielanych przez ludzi. Rzeczywistość społeczna jest konstruktem intelektualnym.

Konstruktywiści uważają, że podstawowym elementem intelektualnym są intersubiektywne przekonania (np. idee, koncepcje, założenia) powszechnie podzielane przez ludzi. Oznacza to, że świat społeczny jest światem ludzkiej świadomości, a więc myśli, wierzeń, idei i koncepcji, języków i dyskursów, znaków, sygnałów i interpretacji funkcjonujących wśród ludzi, którzy go stworzyli, w szczególności wśród grup, jakimi są narody i państwa jako zbiorowe instytucje społeczne.

Zdaniem konstruktywistów kluczem do zrozumienia bezpieczeństwa różnych podmiotów jest uchwycenie jego subiektywnych aspektów, dokonujące się dzięki własnemu doświadczeniu komunikacyjnemu pozwalającemu nam zrozumieć ich tożsamość, postrzeganie zagrożenia i podejmowanie działań ochronnych. W ujęciu konstruktywistycznym bezpieczeństwo jest traktowane jako swoisty konstrukt społeczny.

Specyficzne, autonomiczne miejsce w schemacie badań konstruktywistycznych zajmuje tzw. szkoła kopenhaska[158], stworzona przez grupę uczonych skupionych wokół Barry'ego Buzana i Ole Wævera[159].

Obiektywnie należy przyjąć, że nieco inne założenia strategii bezpieczeństwa były w końcu XX w., a zupełnie odmienne przyjęto po 11 września 2001 r. Od tej daty priorytetem stała się wojna z międzynarodowym (światowym) terroryzmem jako misja, która *de facto* wychodzi poza obronę interesów tylko Stanów Zjednoczonych. Strategia USA zakłada m.in. działania jednostronne w ramach sojuszu północnoatlantyckiego lub partnerstwa, a także współpracę z organizacjami międzynarodowymi w celu umacniania własnego bezpieczeństwa, powiększania potencjału i promowania demokracji.

Ta strategia nie ogranicza działań tylko do fizycznych granic Stanów Zjednoczonych. Wręcz przeciwnie, jej powodzenie opiera się na dążeniu do powiększania wspólnoty narodów bezpiecznych, demokratycznych i stosujących zasady wolnego rynku. Bardzo często

w literaturze występuje stwierdzenie, że na progu XXI w. jedynym gwarantem bezpieczeństwa globalnego i pokoju światowego są Stany Zjednoczone. Jeśli przyjąć historyczny spór między realistami a idealistami w latach 90. XX w., to zwolennicy nurtu teorii neoliberalnych dostrzegli zmiany zachodzące w instytucjach oraz wzajemnych relacjach między instytucjami a rządami narodowymi. W ich koncepcjach instytucje traktowane są instrumentalnie jako środek do uzyskania oczekiwanego celu, czemu towarzyszy ograniczenie suwerenności. W stosunkach zewnętrznych rząd przekazuje pewne kompetencje na poziom międzynarodowy lub ponadnarodowy, jak to stało się w Unii Europejskiej, traktując wynikające z tego ograniczenie suwerenności jako koszt uzyskania oczekiwanych efektów.

Przejawem tradycyjnie pojmowanej mocarstwowości jest kontynuowanie spotkań najpierw w obrębie G-7, siedmiu najbardziej rozwiniętych państw świata, a następnie G-8 z udziałem Rosji. Decyzją mocarstw Rosja została przyjęta do tego grona nie ze względu na jej potencjał i rozwój gospodarczy, ale na jej wciąż ogromne siły militarne wyposażone w broń jądrową. Inne czynniki także świadczą o tym, że obok tradycyjnych przejawów mocarstwowość podlega również pewnej ewolucji, której przebieg od czasu upadku systemu bipolarnego doprowadził do kilku nowych zjawisk. Pierwszym jest rozwój czynników ograniczających samowolę państw zgodnie z prawem międzynarodowym. Jednym z czynników jest tu wzrost liczby i znaczenia organizacji międzynarodowych. Ich niezależność, wsparta nieskrępowaną dociekliwością mediów, jest w stanie nadać rozgłos zjawiskom, w których sprawie mocarstwa wolałyby zachować milczenie. Światowa opinia publiczna, zwłaszcza w krajach demokratycznych, staje się siłą polityczną, z którą władze mocarstw muszą się liczyć.

W okresie po wygaśnięciu antagonizmu Wschód–Zachód zarówno neorealiści, jak i neoliberałowie przewidywali odmienne warianty dla funkcjonowania NATO. Neorealiści pozostawali zwolennikami rozwiązania sojuszu po zniknięciu zagrożenia zewnętrznego, neoliberałowie natomiast opowiadali się za ewolucją, przekształceniem oraz dostosowaniem paktu do nowej sytuacji, a

także rozszerzeniem jego funkcji oraz obszaru działania przez nawiązanie stosunków z państwami Europy Środkowej i Wschodniej[160]. NATO przetrwało i potwierdziło, że łatwiej przystosować istniejącą już organizację do nowej sytuacji, niż utworzyć nową o podobnych celach.

W wieku XXI cechami, które wyróżniają międzynarodowy system bezpieczeństwa utrzymujący się od kilkunastu lat, są niejasność, niepewność i nieprzewidywalność. Dla małej i średniej wielkości państw mocarstwa stanowią ważny czynnik stabilizujący porządek międzynarodowy przez działania polityczne i gospodarcze oraz operacyjne możliwości coraz droższych sił militarnych szybkiego reagowania. Istnienie tych państw jest niejako związane z ewolucją mocarstw i supermocarstw w dzisiejszym świecie. Dlatego instytucjonalna i funkcjonalna rola mocarstw w stosunkach międzynarodowych stała się jednym z najważniejszych problemów analiz i ocen ośrodków politologicznych w tych państwach[161].

Mocarstwa stały się pierwszymi wśród czuwających nad stabilizacją międzynarodową, a przywilej bycia hegemonem sprawia, że inne państwa oczekują wzięcia na siebie społecznego i militarnego bezpieczeństwa zbiorowego. To właśnie one jako pierwsze udzielają największej pomocy humanitarnej i ponoszą największe koszty finansowe i polityczne – za powodzenie lub fiasko operacji – a niekiedy ludzkie wskutek udziału dużej siły militarnej w tego rodzaju misjach. W dzisiejszych czasach bycie mocarstwem stało się kosztowne, ponieważ status ten dostarcza coraz mniej przywilejów i korzyści, a nakłada więcej obowiązków i odpowiedzialności, a także ponoszenia większych kosztów i liczenia się z krytyką w razie niepowodzeń, których nie można wykluczyć. Bogactwo i potęga militarna państw są zjawiskami względnymi, porównywanymi z bogactwem i siłami militarnymi innych państw w czasie[162].

Dynamiczny proces zmian układów sił za każdym razem powodował wyniszczające wojny, które były etapem końcowym przesunięć sił w wyniku długotrwałych procesów rozwoju gospodarczego i społecznego. Zmiana układu sił po zimnej wojnie, w

odróżnieniu od poprzednich tego typu procesów, poddawanych ocenie w ciągu kilkuset lat, odbywała się na drodze pokojowego bilansowania sił i ustaleń, z wykorzystaniem instytucjonalnych form międzynarodowego bezpieczeństwa zbiorowego, co może stanowić wzorzec postępowania mocarstw w polityce bezpieczeństwa w XXI w. Nie wojny, lecz pokojowa współpraca państw o różnych systemach polityczno-społecznych stanowi model porządku międzynarodowego, w którym najważniejszą rolę odgrywają mocarstwa[163].

Na obecne kryzysy, zagrożenie terroryzmem, cyberterroryzmem i bronią nuklearną, a także problemy ekologiczne, ruchy migracyjne czy problemy gospodarki światowej nie widać jednoznacznych odpowiedzi. W konfrontacji ze światem współczesnym liberałowie są podzieleni, jeżeli chodzi o interwencję w sprawy innych państw. Powstaje bowiem pytanie, czy powinno się to czynić w imię demokracji i praw człowieka, czy też powstrzymać się od interwencji w imię zasady samostanowienia i suwerenności[164]. Obserwując obecną politykę międzynarodową, można zauważyć wiele podziałów, postaw i priorytetów. Niekiedy nie da się jednoznacznie sklasyfikować sposobu działania głównych aktorów sceny międzynarodowej, a filozoficzne koncepcje w konfrontacji ze światem współczesnym nie zawsze się sprawdzają. Refleksja na temat podziału w stosunkach transatlantyckich zdaje się nie zamykać w ramach podziału na idealizm i realizm. Dynamicznie zmieniająca się rzeczywistość i wielorakie tendencje dają efekt trudny do przewidzenia. Choć amerykański sposób sprawowania polityki budzi falę krytyki w Europie i odwrotnie, to istnieje szansa na porozumienie. Jest ona tam, gdzie zabiegi o uczynienie świata bezpiecznym dla demokracji spotykają się z zabiegami o zapewnienie światu bezpieczeństwa dla obu podmiotów nawzajem[165].

W rozwoju społecznym państwa należy postrzegać zagrożenia, które mogą paraliżować życie społeczne. Najogólniej możemy je identyfikować ze stanem charakteryzującym się destabilizacją ładu politycznego, zahamowaniem przeszkód we współpracy w sojuszach

UE i NATO, istotnym osłabieniem pozycji międzynarodowej, zahamowaniem rozwoju cywilizacyjnego narodu i społeczeństwa. Te obszary zagrożeń mają społeczne tło. Mogą być wynikiem destrukcyjnych procesów zachodzących w społeczeństwie, a przez to destabilizować strukturę społeczną, a także tworzyć niekorzystne uwarunkowania do wypełniania funkcji przez państwo.

Pierwsza *Europejska strategia bezpieczeństwa* została określona i przyjęta w imieniu UE i przywódców państw członkowskich przez Wysokiego Przedstawiciela ds. Wspólnej Polityki Zagranicznej i Bezpieczeństwa podczas brukselskiego posiedzenia Rady Europejskiej 12 grudnia 2003 r.[166] Strategia ta jest krokiem milowym w zakresie polityki bezpieczeństwa Unii, gdyż po raz pierwszy państwa europejskie zdecydowały się zdefiniować potencjalne zagrożenia i określiły działania mogące przeciwdziałać ich powstaniu[167]. We wprowadzeniu m.in. stwierdza, że „jako związek 25 państw liczących ponad 450 milionów ludzi oraz wytwarzający ponad jedną czwartą światowego produktu brutto, dysponujący szeroką paletą instrumentów, Unia Europejska staje się w sposób nieunikniony globalnym graczem".

Konstruując *Europejską strategię bezpieczeństwa*, państwa członkowskie wyszły od stwierdzenia, że środowisko po zimnej wojnie charakteryzuje się coraz szerszym otwarciem granic, co spowodowało trwałe powiązanie wewnętrznych i zewnętrznych aspektów bezpieczeństwa. Jako główne zagrożenia bezpieczeństwa strategia wymienia terroryzm, proliferację broni masowego rażenia, konflikty regionalne, upadek lub rozkład państw oraz przestępczość zorganizowaną.

Z kolei cele strategiczne UE sformułowano w drugiej części ESB w postaci trzech elementów. Pierwszym są odpowiedzi na zagrożenia wymieniające reakcję organizacji na wydarzenia z 11 września i użycie różnych środków, np. przyjęcie europejskiego nakazu aresztowania (ENA). Przywołano uzgodnienie polityki przeciwdziałania rozprzestrzenianiu broni masowego rażenia oraz przyjęcie dalszego programu działania, przewidującego kroki w kierunku wzmocnienia Międzynarodowej Agencji Energii Atomowej,

a także uruchomienie środków dotyczących kontroli eksportu, przemytu i nielegalnej produkcji broni[168]. Drugim celem strategicznym UE jest budowanie bezpieczeństwa w sąsiedztwie, trzecim – porządek międzynarodowy oparty na skutecznym multilateralizmie. Zadeklarowano, że bezpieczeństwo i pomyślność Europy w coraz większym stopniu zależy od efektywnego systemu współpracy wielostronnej, a Unia Europejska przywiązana jest do utrzymania i rozwoju prawa międzynarodowego[169].

Choć zdecydowana większość analityków podkreśla historyczny wymiar oraz znaczenie strategii dla rozwoju UE i kształtowania jej tożsamości, to pojawiły się wnioski, że stanowi ona bardziej wizję niż zbiór strategicznych interesów, w większym stopniu wskazując postawę Unii niż jej zasady polityczne w obszarze bezpieczeństwa. Jej kształt wynika bowiem z faktu, że powstanie tego dokumentu poprzedzały trudne niekiedy rokowania, a efekt końcowy stał się wynikiem kompromisu zawartego między państwami członkowskimi[170].

Mimo że przewiduje się przykładowo użycie siły zbrojnej w walce z terroryzmem, to zasady jej wykorzystania nie zostały określone. Wspomina się jedynie, że rozwijana przez Unię Europejską wspólna polityka bezpieczeństwa i obrony musi się przyczyniać do zwalczania tego zagrożenia, ale ustalenie precyzyjnych zasad użycia siły jest szczególnie ważne w sytuacji, kiedy Unia zadeklarowała ścisłą współpracę w zwalczaniu terroryzmu ze Stanami Zjednoczonymi.

W 2008 r. w swoim raporcie dotyczącym wdrażania strategii bezpieczeństwa zewnętrznego (SBZ) Javier Solana zauważył nowe typy zagrożeń, takie jak bezpieczeństwo energetyczne czy cyberbezpieczeństwo[171]. Przyczyną ich ujawnienia i pogłębienia było wejście w życie Traktatu z Lizbony, kryzys gospodarczy UE, Arabska Wiosna, kryzys ukraiński oraz nasilenie się działalności ISIS. To z kolei doprowadziło do fragmentaryzacji bezpieczeństwa w Europie objawiającej się m.in. mechanizmem nordyckim czy współpracą francusko-brytyjską[172]. Zdaniem Solany konieczne było wdrożenie istniejących instrumentów ONZ dotyczących przestępczości zorganizowanej czy terroryzmu. Brak harmonizacji prawa z poziomu

wspólnotowego na poziom krajowy doprowadził do tego, że postęp był powolny i niekompletny, dlatego konieczna jest lepsza koordynacja, przejrzystość i elastyczność różnych agencji na szczeblach krajowym i europejskim. Ponadto UE powinna dalej wzmacniać partnerstwo antyterrorystyczne z USA w zakresie udostępniania danych i ochrony.

Szybki rozwój technologii informacyjnych i komunikacyjnych (ICT), a w szczególności cyfrowa konwergencja usług, sieci i urządzeń, wyraźnie wpływająca na wzrost gospodarczy i zatrudnienie, stają się coraz istotniejszym elementem gospodarki i społeczeństwa. Odpowiedzią na zachodzące zmiany powinna być – zdaniem Komisji Europejskiej – proaktywna polityka, nakierowana na uzyskanie spójności między przyjętymi ramami regulacyjnymi a nowo powstałą gospodarką cyfrową. Aby to uzyskać, Komisja opracowała strategiczne podejście do zagadnień społeczeństwa informacyjnego i mediów audiowizualnych. W komunikacie z 1 czerwca 2005 r.[173] *i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia* Komisja wskazała trzy priorytety polityki w tej dziedzinie: ukończenie jednolitej europejskiej przestrzeni informacyjnej, wzmocnienie innowacji i inwestycji w badaniach nad ICT oraz stworzenie integracyjnego europejskiego społeczeństwa informacyjnego.

Zdaniem Komisji jednym z celów polityki europejskiej powinno być utworzenie jednolitej europejskiej przestrzeni informacyjnej zapewniającej bezpieczną łączność szerokopasmową po przystępnych cenach, bogatą i zróżnicowaną zawartość oraz usługi cyfrowe. Działania podejmowane w tym celu powinny się odnosić do czterech najważniejszych elementów: szybkości (upowszechnienia szybkich usług szerokopasmowych), zawartości multimedialnej (poprawa pełności ekonomicznej i prawnej sprzyjająca powstawaniu nowych usług i zawartości online), interoperacyjności (zapewnienie komunikacji między różnymi platformami a urządzeniami) oraz bezpieczeństwa (zwiększenie zaufania konsumentów do nowych technologii przez ochronę Internetu przed oszustwami, szkodliwymi treściami oraz awariami technologicznymi). Komisja podkreśliła

konieczność przeprowadzenia przeglądu ram regulacyjnych dotyczących łączności elektronicznej, opracowania i wdrożenia strategii na rzecz bezpieczeństwa europejskiego społeczeństwa informacyjnego. Zwrócono także uwagą na potrzebę stworzenia spójnych ram rynku wewnętrznego usług audiowizualnych, w tym unowocześnienie ram prawnych oraz wspieranie wprowadzenia w życie istniejącego *acquis* dotyczącego usług w tym obszarze[174].

Kolejnym wskazanym przez Komisję priorytetem są innowacje i inwestycje w badania. Celem w tym obszarze jest osiągnięcie światowego poziomu badań i innowacji w dziedzinie technologii informacyjnych i komunikacyjnych przez zrównanie się z głównymi konkurentami Europy. Działania podejmowane przez Komisję w tym zakresie mają polegać m.in. na wspieraniu badań strategicznych nad ICT, zachęcaniu podmiotów prywatnych do inwestycji w tym obszarze i znoszeniu barier technologicznych, organizacyjnych oraz prawnych utrudniających wdrożenie ICT i przez to negatywnie wpływających na uzyskanie lepszych wyników badań do osiągnięcia korzyści ekonomicznych. Środki zastosowane w tym obszarze mają zachęcać do przekładania postępu technologicznego na innowacyjne zastosowania w sektorze publicznym i prywatnym. Badania strategiczne mają głównie dotyczyć technologii służących wiedzy, zawartości i kreatywności, otwartych sieci łączności, bezpiecznego i niezawodnego oprogramowania, systemów wbudowanych oraz nanoelektroniki.

Następnym priorytetowym obszarem, opisanym w strategii *i2010*, jest integracja społeczna, lepsze usługi i wyższa jakość. Zwrócono szczególną uwagę na konieczność upowszechniania produktów i usług ICT, również w regionach słabiej rozwiniętych. Komisja zobowiązała się do przedstawienia wytycznych politycznych na temat e-dostępności i zasięgu usług szerokopasmowych, przyjęcia planu działania na rzecz elektronicznej administracji oraz ustanowienia wzorcowych inicjatyw ICT w zakresie jakości życia.

W podsumowaniu strategii *i2010* zaakcentowano, że dzięki jej wprowadzeniu Europa stanie się atrakcyjniejszym miejscem dla inwestycji i innowacji w dziedzinie towarów i usług opartych na

wiedzy. Podkreślono ważną rolę każdego z podmiotów odpowiedzialnych za jej realizację: Komisji Europejskiej – realizującej przedstawione zadania, państw członkowskich – wprowadzających nowe ramy regulacyjne i podejmujących własne inicjatywy w tym obszarze, a także pozostałych podmiotów odpowiedzialnych za prowadzenie otwartego i konstruktywnego dialogu[175].

Na tle ewoluujących dynamicznie zagrożeń i w związku z faktem uznania cyberterroryzmu za kolejne ważne wyzwanie Unii Europejskiej przyjęto najpierw 25 czerwca 2013 r. strategię UE[176] na rzecz bezpieczeństwa cybernetycznego, w której głównymi celami były promocja zarówno poprawy cyberbezpieczeństwa w całej Unii i poza nią, jak i międzynarodowej współpracy w zakresie cyberbezpieczeństwa.

Strategia uwzględniająca nadrzędną wartość, jaką jest niezbywalne prawo człowieka do poszanowania jego godności, w tym również prawo do swobodnego wypowiadania swoich myśli i opinii, oparta jest na kilku priorytetach.

Pierwszym kluczowym obszarem opisanym w strategii z 2013 r. jest dobrobyt jednolitego rynku cyfrowego oraz podkreślenie znaczenia najnowszej technologii informacyjnej i komunikacyjnej UE (ICT) oraz sektor bezpieczeństwa ICT w odniesieniu do wzmocnienia cyberbezpieczeństwa. Podkreśla, że prawodawstwo powinno wspierać innowacje i wzrost gospodarczy, badania naukowe oraz koncentrować się na ochronie infrastruktury, ponieważ gospodarka cyfrowa jest główną siłą napędową wzrostu, innowacji i zatrudnienia, a cyberbezpieczeństwo ma kluczowe znaczenie dla ochrony gospodarki cyfrowej.

Drugim wskazanym obszarem jest osiągnięcie odporności cybernetycznej za pomocą środków służących poprawie bezpieczeństwa sieci i informacji w całej Unii na poziomie państw członkowskich, współpraca między państwami członkowskimi i w całej UE. Podkreśla się tu rolę zespołu reagowania na incydenty komputerowe (CERT) i Agencji Unii Europejskiej ds. Bezpieczeństwa

Sieci i Informacji (ENISA) oraz zachęca ENISA do współpracy z instytucjami państwowymi.

Zauważono, że należy zwiększyć unijną odporność infrastruktury krytycznej i wzmocnić ją przez ścisłą współpracę i koordynację między odpowiednimi podmiotami, także między cywilnymi a europejskimi podmiotami wojskowymi. Konieczne jest również wzmocnienie ścisłej współpracy i koordynacji w reagowaniu na incydenty cybernetyczne przez podmioty obrony, organy ścigania, sektor prywatny i cyberorgany bezpieczeństwa, aby skutecznie stawić czoło wyzwaniom cybernetycznym.

Za trzeci priorytet uznano zwalczanie cyberprzestępczości, choć jednocześnie zaznaczono, że ma on najważniejsze znaczenie w obszarze polityki ochrony bezpieczeństwa w Internecie. W związku z tym należy wspierać państwa członkowskie na ich wniosek w określaniu luk i wzmacnianiu ich zdolności w celu prowadzenia polityki prewencyjnej i zwalczania cyberprzestępczości, korzystać z Funduszu Bezpieczeństwa Wewnętrznego (ISF) w ramach limitu jego budżetu w celu wsparcia odpowiednich organów zwalczających cyberprzestępczość, korzystać z Instrumentu na rzecz Stabilności (IfS) w celu rozwijania walki z cyberprzestępczością, rozwijać inicjatywy budujące potencjał, w tym współpracę policyjną i sądową w krajach trzecich z miejsc, w których działają organizacje cyberprzestępcze.

Czwartym obszarem jest *Wspólna polityka bezpieczeństwa i obrony* (WPBiO). W tym przypadku głównym zadaniem jest opracowanie ram cyberobrony i określenie konkretnych kroków w sprawie bezpieczeństwa i obrony przez zwiększenie zdolności państw członkowskich do obrony cybernetycznej, wykorzystanie istniejących mechanizmów łączenia i udostępniania oraz wykorzystywania synergii z szerszej polityki UE mające na celu zbudowanie niezbędnych zdolności w zakresie obrony cybernetycznej w państwie członkowskim. W tej sytuacji konieczne było przyjęcie nowej strategii bezpieczeństwa zewnętrznego UE.

2.3
ISTOTA STRATEGII OCHRONY CYBERPRZESTRZENI UNII EUROPEJSKIEJ

Na wstępie tego podrozdziału należy się zastanowić, czy polityka bezpieczeństwa może funkcjonować bez strategii. Nie ulega wątpliwości, że politycy i wielcy menedżerowie mają znaczący wpływ, obok innych czynników, na kształtowanie strategii bezpieczeństwa, a więc twórczo biorą udział w określaniu, czym jest strategia[177].

Jaką rolę odgrywa strategia w polityce bezpieczeństwa w różnych dziedzinach oraz czy polityka może funkcjonować bez strategii bezpieczeństwa? Odpowiedź na tak postawione pytanie może ułatwić formułowanie odpowiedzi na pozostałe wątpliwości. Może ona być prosta i jednoznaczna – polityka bez strategii lub polistrategii może istnieć, a stawiane cele mogą być dalekosiężne, ale nie zostaną zrealizowane.

Przyczyna takiego stanu rzeczy leży głównie w strategii, tj. w metodach i sposobach oraz narzędziach wykonania. Upraszczając odpowiedź, możemy powiedzieć, że strategia jest „narzędziem" polityki, a jeśli tak, to w moim przekonaniu, definicja strategii może przyjąć następującą postać: „Strategia bezpieczeństwa to sposoby tworzenia i stosowania skutecznych systemów reagowania na wszelkie zagrożenia dla osiągnięcia długofalowych celów". Odpowiadając na pytanie, jakie miejsce zajmuje strategia w polityce, możemy stwierdzić, że zajmuje ona miejsce znaczące, czyli zasadnicze[178].

W modelowym funkcjonowaniu systemu bezpieczeństwa narodowego bądź międzynarodowego polityka określa długofalowe cele w danym obszarze, strategia zaś wyznacza konkretne sposoby i metody oraz środki ich realizacji. Relacje te są szczególnie bliskie na etapie projektowania, czyli w warstwie celów. Polega to na tym, że cele polistrategii, która powinna być narzędziem realizacji ogólnej polityki państwa w sprawach bezpieczeństwa narodowego, w

znacznej mierze mają być wyrazem tych celów polityki państwowej, które odnoszą się do zewnętrznej aktywności państwa[179]. Właśnie dlatego istnieje potrzeba zapewnienia skoordynowanego wpływu najważniejszych organów państwa na działanie strategii, które odpowiadają za bezpieczeństwo, w reakcji na współczesne zagrożenia. Wszystko to przemawia za potrzebą prowadzenia coraz głębszych analiz badawczych, które będą brały pod uwagę zjawisko łączenia polityki ze strategią i strategii z polityką w obszarze bezpieczeństwa narodowego, regionalnego i globalnego[180].

Od niedawna w literaturze pojawił się nowy termin – strategia pokojowa (pokoju). Dla podkreślenia celowości wyodrębnienia strategii pokoju przytoczę poglądy Garetha Evansa[181], który proponuje cztery strategie reakcji:

- strategia budowania pokoju,
- strategia zachowania pokoju,
- strategia wymuszania pokoju,
- strategia przywrócenia pokoju.

Strategia budowania pokoju ma na celu niedopuszczenie do powstawania sporów, konfliktów zbrojnych i innych poważnych kryzysów bezpieczeństwa, a strategia zachowania pokoju – rozwiązanie lub ograniczenie poszczególnych sporów oraz pewnych potencjalnych zagrożeń, aby nie dopuścić do konfliktu zbrojnego z powodów politycznych lub innych. Istotą strategii wymuszania pokoju jest reakcja na konflikty lub inne poważne kryzysy bezpieczeństwa, kiedy nie ma porozumienia. Strategia przywrócenia pokoju jest natomiast stosowana po konflikcie zbrojnym, jeśli strony konfliktu wyrażają zgodę na współpracę pokojową. Uwzględniając zasadniczą treść tych czterech strategii reakcji na zagrożenia bezpieczeństwa kooperatywnego, można zdefiniować strategię pokojową następująco: „Strategia pokojowa to teoria i praktyka przygotowania i wykorzystania będących w dyspozycji zasobów w celu poprawnego układania stosunków między państwami, zgodnie z zasadami współżycia międzynarodowego”.

Następną cechą polistrategii, jak zauważa Paweł Soroka[182], powinna być jej synergiczność. Ta cecha oznacza zdolność do skutecznego koordynowania sposobów i metod postępowania w trakcie realizacji zadań charakterystycznych dla poszczególnych sektorowych strategii bezpieczeństwa narodowego. Chodzi głównie o to, aby się one wzajemnie wzmacniały i sumowały, dając pozytywny – synergiczny efekt końcowy[183]. Kolejną cechą jest jej profilantyczność, która polega na wyprzedzaniu zjawisk i wydarzeń rozgrywających się w otoczeniu geopolitycznym. W tym przypadku można z wyprzedzeniem inspirować działania prewencyjne wobec zagrożeń bezpieczeństwa państwa. Ponadto do tej części polistrategii należy jej aktywność na arenie międzynarodowej i reagowanie na zagrożenia zgodnie z przyjętymi celami. Do cech polistrategii należy również mobilizacyjność, wyrażająca się z jednej strony wywieraniem przez sferę realizacyjną skutecznego wpływu na wszystkie instytucje narodowe i międzynarodowe oraz organizacje pozarządowe będące instrumentami strategii sektorowych, z drugiej – założeniem, że strategie sektorowe będą komplementarne z nią jako strategią nadrzędną. Nie mniej ważną cechą polistrategii jest jej państwowocentryczny charakter mimo wzrostu znaczenia podmiotów niepaństwowych. Cecha ta oznacza zwiększenie roli ochrony podstawowych wartości państwa, tj. bezpieczeństwa i rozwoju, a realizacja tego należy do państwa.

Sektorowe strategie powinny natomiast należeć do resortów konstytucyjnych, ponieważ każdy z nich ma własną strategię rozwoju, w zależności od jego specyfiki, a polistrategia bezpieczeństwa państwa powinna się charakteryzować szerokim zakresem przestrzennym. Zakres ten powinien być znacznie szerszy niż zakres przestrzenny poszczególnych strategii sektorowych. Obejmuje on wszystkie zakresy działań realizowanych przez strategie sektorowe i w zasadzie – ze względu na zasięg i rodzaj niektórych zagrożeń – powinien aktualnie mieć zakres globalny, a nie tylko regionalny[184].

Po rozszerzeniu Unii Europejskiej szczególnego znaczenia nabrał wymiar europejski polistrategii bezpieczeństwa. Ostatnią jej cechą

jest kooperatywność, która przejawia się tym, że w warunkach rosnącej współzależności między państwami i jednocześnie pojawienia się zagrożeń nie tylko w bliskim środowisku międzynarodowym nasila się konieczność przeciwstawienia się im w kooperacji z innymi państwami. Kooperatywność polistrategii bezpieczeństwa narodowego jest zawsze związana z bezpieczeństwem innych państw, zwłaszcza będących w sojuszu[185]. Na zakończenie rozważań na temat cech polistrategii pragnę podkreślić, że dotyczą one głównie bezpieczeństwa narodowego, zewnętrznego i wewnętrznego. Tylko niektóre z nich wiążą się ze strategią sektorową, co w teorii bezpieczeństwa jest rozumowaniem racjonalnym.

Jak już wspomniano, strategia jest narzędziem polityki, która może istnieć bez strategii lub polistrategii, stawiane cele mogą być dalekosiężne, tylko nie będą zrealizowane. Przyczyna takiego stanu rzeczy leży głównie w strategii, tj. w metodach i sposobach oraz narzędziach wykonania. Strategią bezpieczeństwa są sposoby tworzenia i stosowania skutecznych systemów reagowania na wszelkie zagrożenia dla osiągnięcia celów długofalowych.

Strategia bezpieczeństwa informacyjnego dotyczy przede wszystkim zasobów informacyjnych, które wiążą się ze zdobywaniem informacji, przekazywaniem, przechowywaniem i udostępnianiem ich. Powszechna dostępność do informacji, poza jej pozytywnymi aspektami, powoduje również występowanie licznych nowych uwarunkowań w dobie rozwoju wielu dziedzin. W warunkach współczesnych będą mieli przewagę tylko ci, którzy będą dysponowali wszechstronną, aktualną i wiarygodną informacją. Oznacza to, że mając dostęp do informacji wszelkiego rodzaju, w zależności od konkretnych potrzeb, można wygrać z potencjalnym przeciwnikiem w każdym zakresie działalności, w obszarze wewnętrznego i zewnętrznego bezpieczeństwa państwa[186]. Informacyjne oddziaływanie na zachowania i postawy podmiotów międzynarodowych i krajowych, ochrona interesów narodowych przed negatywnymi skutkami oddziaływań tych podmiotów powinny być koordynowane w ramach polityki rządu, natomiast w sferze

wykonawczej – w strategii sektorowej bezpieczeństwa wewnętrznego państwa. W tym przypadku byłaby ona związana z bezpieczeństwem narodowym, a zwłaszcza z ochroną porządku konstytucyjnego, bezpieczeństwem militarnym, publicznym, ekonomicznym i społecznym.

Współczesna cywilizacja opiera swą działalność na szeroko pojętej informacji. To oznacza, że korzystanie z niej jest dzisiaj oczywiste. Informacja, która jest podstawą wiedzy, staje się istotnym elementem w osiąganiu sukcesu, dlatego nabiera szczególnego znaczenia w każdej dziedzinie działalności człowieka. Informacje są czymś pozytywnym w życiu i działalności człowieka w każdym obszarze. Oceniając je w różnych aspektach, należy podkreślić, że mogą być także – w odmiennych sytuacjach – zagrożeniem dla jednostki, grupy społecznej, państwa powodowanym przez osoby, działalność obcych państw lub organizacji terrorystycznych. Takie negatywne wykorzystywanie informacji przeciwko innemu podmiotowi jest dzisiaj powszechne.

Strategia bezpieczeństwa kulturowego odnosi się do zagrożeń zewnętrznych, a jednocześnie do wartości duchowych danego narodu, do wartości integrujących naród, do symboli[187]. Skomplikowane relacje między globalizacją a elementami narodowymi i lokalnymi przynoszą różne skutki – pozytywne i negatywne, mogą być szansą, a jednocześnie zagrożeniem. Należy tu także dostrzegać takie zjawiska, jak nierzadkie przypadki wykorzystywania kultury masowej przez kultury lokalne, etniczne i religijne posługujące się mediami elektronicznymi i Internetem. Niewątpliwie zagrożenia w obszarze kultury materialnej są bardziej uchwytne niż w kulturze symbolicznej, a tym samym łatwiejsze jest określenie stanu bezpieczeństwa kulturowego w tym sektorze[188].

Strategie cyberbezpieczeństwa[189], czyli metody realizacji polityki bezpieczeństwa systemu informacyjnego, są adaptacjami metod stosowanych w szeroko pojętej problematyce bezpieczeństwa życia społecznego. Kilka z nich jest obecnie uznawanych za standardowe w problematyce bezpieczeństwa informacyjnego, dlatego trzeba je scharakteryzować.

Należy do nich wielowarstwowa kontrola dostępu do systemu informatycznego, która zakłada, że uwierzytelnianie użytkownika będzie przebiegać w kilku etapach, zwanych warstwami ochrony systemu teleinformatycznego. Pierwszą warstwę ochrony tworzą fizyczne urządzenia zabezpieczające, a więc zakratowanie okien w pomieszczeniach ze sprzętem teleinformatycznym, wyposażanie tych pomieszczeń w drzwi z metalowym okuciem, zainstalowanie alarmu, zamontowanie w drzwiach zamków otwieranych za pomocą kart magnetycznych lub kart elektronicznych. Dostęp do pomieszczeń z systemami informatycznymi, wymagającymi najwyższego poziomu bezpieczeństwa, powinien być dodatkowo nadzorowany przez pracowników ochrony organizacji. Kolejną popularną warstwą ochrony jest procedura uwierzytelniania użytkownika przed rozpoczęciem pracy w systemie. Identyfikacja użytkownika może obejmować sprawdzenie trzech podstawowych warunków rejestracji: hasła (posiadanie przez użytkownika odpowiedniej wiedzy), żetonu (posiadanie przez użytkownika odpowiedniego przedmiotu, np. karty magnetycznej lub elektronicznej) i danych biometrycznych, np. linii papilarnych (posiadanie odpowiednich cech fizycznych). Połączenie tych elementów umożliwia zastosowanie uwierzytelniania wieloetapowego, które jednoznacznie potwierdza tożsamość użytkownika.

Kolejną warstwą ochrony jest hierarchizacja uprawnień użytkowników, która zakłada, że użytkownicy systemu otrzymują różne uprawnienia. Najszersze uprawnienia mają administratorzy systemu, mniejsze natomiast – administratorzy podsystemów. Najmniejsze uprawnienia są przydzielane zwykłym użytkownikom. Obowiązuje zasada przyznawania minimum uprawnień dla stanowiska. W konsekwencji, jeśli wystąpi zagrożenie systemu, będzie ono dotyczyć tylko fragmentu systemu i zawężonego kręgu użytkowników.

Innym typem zabezpieczenia jest wskazywanie i monitorowanie miejsc wymiany informacji systemu teleinformatycznego z otoczeniem. Zgodnie z tą strategią każda wymiana informacji między systemem teleinformatycznym organizacji a siecią globalną

odbywa się przez wydzielony fragment systemu pracujący pod kontrolą specjalnego oprogramowania. Program ten ma za zadanie monitorować przesyłane informacje i sygnalizować wszelkie nieprawidłowości oraz fakty mogące grozić bezpieczeństwu systemu organizacji.

Przykładem realizacji tej strategii jest system CheckPoint FireWall-1. Umożliwia on stworzenie rozproszonej architektury kontroli przesyłania informacji. W sieci można zainstalować kilka modułów zapory ogniowej (firewalli), z których każdy może pracować w innym systemie operacyjnym, a wszystkie te moduły mogą być zarządzane centralnie, z jednego węzła sieci. Dzięki temu możliwe jest opracowanie wspólnej polityki bezpieczeństwa dla dużej sieci teleinformatycznej. System CheckPoint FireWall-1 umożliwia zdefiniowanie polityki bezpieczeństwa sieci w postaci zbioru reguł, z których każda opisuje sposób kontrolowania transmisji w ustalonym punkcie sieci. Moduły zapory ogniowej, poza filtrowaniem, pozwalają na rejestrowanie i przeglądanie zdarzeń. Automatyczne blokowanie systemu w przypadku wykrycia włamania poleca automatyczne blokowanie systemu teleinformatycznego lub jego części w przypadku wykrycia zagrożenia. Blokowanie ma na celu uniemożliwienie intruzowi wyrządzenia szkód. Ponadto w momencie wykrycia zagrożenia system powinien zapisać swój stan w pamięci zewnętrznej. Ułatwia to znalezienie wyłomu w systemie bezpieczeństwa i likwidację ewentualnych szkód[190].

Wojna cybernetyczna jest częścią wojny informacyjnej. Przestrzeń informacyjną (infosferę) stanowi ogół informacji dostępnych człowiekowi. Cyberprzestrzeń (cybersfera) to jej specyficzna część. Według niektórych koncepcji pojęcie cyberwojny zostało utworzone przez siły zbrojne dla określenia kolejnego, wirtualnego tym razem pola walki. Istotę wykorzystania cyberprzestrzeni do prowadzenia wojny – walki informacyjnej – najpełniej prezentuje pierścieniowy model Johna Wardena. Po wojnie w Zatoce (1991) płk John Warden opracował zasady użycia lotnictwa do prowadzenia wojny strategicznej przeciwko środkom ciężkości przeciwnika. Twierdził on, że wszyscy przeciwnicy mogą być postrzegani jako systemy

celów, składające się z pięciu środków ciężkości tworzących koncentryczne pierścienie. Zgodnie z tą koncepcją łańcuchową istnieje możliwość wywarcia presji na przywódców, zagrażając ich systemom, przez atakowanie najwrażliwszych środków ciężkości i pomijanie sił zbrojnych przeciwnika. Najbardziej krytycznym pierścieniem spośród wszystkich pięciu zawartych w jego modelu jest przywództwo, następnie źródła zaopatrzenia, dalej infrastruktura państwa, później ludność, a na końcu siły zbrojne. Dostęp tych systemów jest odwrotny do ich ważności. Przy analizie podatności na atak najważniejszych środków ciężkości poszczególnych obszarów infrastruktury systemu obronnego państwa wykorzystuje się kręgi Wardena. Można łatwo zauważyć, że ataki w cyberprzestrzeni są w stanie przeniknąć w głąb pierścieni i zaatakować wybiórczo wnętrze dowolnego pierścienia, bez wcześniejszego przebijania się przez pierścienie zewnętrzne.

Zaproponowany przez Wardena model ma charakter uniwersalny i może być wykorzystany do analizy prowadzenia walki informacyjnej. Należy pamiętać, że w wysoko rozwiniętych społeczeństwach uzależnienie od elektroniki staje się swoistą piętą achillesową. Coraz większe uzależnienie od komputerów i Internetu, powstawanie specyficznego cyberświata sprawia, że znawcy tematu zaczęli traktować również cyberprzestrzeń jako nowy, piąty wymiar walki, obok lądu, powietrza, morza i przestrzeni kosmicznej. Colin S. Gray stwierdził: „Obecnie mamy i w przyszłości będziemy mieli do czynienia z co najmniej pięcioma współzależnymi środowiskami wojny: lądem, morzem, powietrzem, kosmosem i cyberprzestrzenią".

Ryzyko strategiczne jest związane z długookresową perspektywą czasową, np. dziesięcioletnią. Jest ono zarezerwowane dla najwyższego kierownictwa. Ze względu na jego kluczową rangę wpływa ono w sposób bezpośredni na możliwości trwania i rozwoju organizacji. W *Leksykonie wiedzy wojskowej* ryzyko strategiczne wyjaśniono jako „podjętą decyzję lub zamierzone działanie na szczeblu strategicznym, przy świadomym uwzględnieniu niepewności osiągnięcia przewidywanych celów o charakterze strategicznym i w związku z tym istnienia niebezpieczeństwa poniesienia porażki". Współcześnie cyberprzestrzeń jest przestrzenią

wzmożonego ryzyka. Im więcej wiedzy, tym bardziej rośnie niepewność i ryzyko, tym bardziej złożone stają się struktury społeczne. Skutkami ubocznymi są kradzież, włamania, spam i wirusy. Zdajemy sobie sprawę, że zwykłe „stukanie" w klawiaturę może przynieść skutki o wysokim stopniu ryzyka. Globalizacja powoduje, by wszyscy bez wyjątku bezustannie nawzajem się obserwowali i porównywali. Odkąd globalizacja stała się faktem, cybernetyka sieci jest nie tyle technologią, ile raczej technosystemem strategicznej komunikacji, którego działanie pociąga za sobą systemowe ryzyko niszczącej wszystko wokół reakcji.

Plan budowy społeczeństwa informacyjnego w Unii Europejskiej zapoczątkowano w 1993 r. w dokumencie *Growth, Competitiveness and Employment. The Challenges and Ways Forward into 21st Century – White Paper*[191]. Za początek rozwoju polityki tworzenia społeczeństwa informacyjnego uznaje się publikację przez Komisję Europejską w 1994 r. dokumentu *Europa i społeczeństwo globalnej informacji*. *Zalecenia dla Rady Europy*. Postulaty zawarte w tym raporcie wyznaczyły politykę Unii Europejskiej w dziedzinie społeczeństwa informacyjnego. Zgodnie z nimi:

- rozwój społeczeństwa informacyjnego powinien kierować wolny rynek, konieczne jest zatem stworzenie warunków uczciwej konkurencji w dziedzinie usług telekomunikacyjnych i informacyjnych,
- konieczne jest zapewnienie na terenie UE powszechnego dostępu do usług, aplikacji, usług i programów informacyjnych,
- środki finansowe przeznaczone na rozwój społeczeństwa informacyjnego powinny pochodzić przede wszystkim z sektora prywatnego,
- niezbędne są ochrona prywatności i bezpieczny przepływ informacji, należy więc zapewnić ochronę i promowanie różnic kulturowych oraz językowych w Unii Europejskiej,
- trzeba podjąć współpracę z krajami mniej rozwiniętymi gospodarczo, w szczególności z krajami Europy Środkowej i Wschodniej,

- należy promować i uświadamiać, jakie nowe możliwości daje rozwój społeczeństwa informacyjnego oraz przeprowadzić odpowiednie szkolenia na wszystkich etapach edukacji.

W 1996 r. Komisja Europejska opublikowała *Green Paper. Living and Working in Information Society. People First*[192]. Dokument ten skupiał się na konsekwencjach, jakie przyniesie obywatelom transformacja w kierunku społeczeństwa informacyjnego, oraz na wpływie ICT na ich życie. Kolejną inicjatywą Unii zmierzającą do budowy nowoczesnej i silnej gospodarki krajów członkowskich był projekt *eEurope – An Information Society for All*[193]. Projekt ten opierał się na kilku priorytetach: edukacji, sektorze zdrowia, aktywizacji zawodowej osób niepełnosprawnych i transporcie. W 1999 r. wydano *Zieloną Księgę Public Sector Information: a Key Resource for Europe*. Dokument ten przedstawiał korzyści zarówno dla obywateli, jak i całej gospodarki, które wynikały z wykorzystania w obszarze służb publicznych technologii telekomunikacyjnych i informatycznych[194].

Priorytetem dla Unii Europejskiej stało się umożliwienie powszechnego dostępu do Internetu. Plan mający na celu budowę europejskiego społeczeństwa informacyjnego został opracowany 23–24 marca 2000 r. w Lizbonie na specjalnym posiedzeniu Rady Europejskiej i zyskał nazwę *Strategii Lizbońskiej*[195]. Opracowano go na dwóch płaszczyznach: gospodarczej i społecznej. Płaszczyzna gospodarcza budowy społeczeństwa informacyjnego miała się opierać na wykorzystaniu ICT w celu zwiększenia konkurencyjności gospodarki, płaszczyzna społeczna natomiast – na koncepcji Luca Soete'a, który uznał społeczeństwo informacyjne za „społeczeństwo, które właśnie się kształtuje, w którym technologie gromadzenia oraz transformacji informacji i danych są powszechnie dostępne po niskich kosztach. Powszechnemu dostępowi do informacji i danych towarzyszą organizacyjne, komercyjne, społeczne i prawne zmiany, które głęboko zmieniają życie, pracę i społeczeństwo jako takie"[196].

W trakcie szczytu europejskiego w Santa Maria de Feira w 2000 r. został przyjęty kolejny plan *eEurope 2002 – An Information Society for All*. Dokument ten wskazywał konieczność rozwoju szybkiego,

taniego, powszechnego Internetu, inwestowania w potencjał ludzki oraz popularyzacji wykorzystania sieci wirtualnej. Następny plan rozwoju społeczeństwa informacyjnego, rozumianego jako strategiczny element budowy gospodarki opartej na wiedzy, przedstawiono w Göteborgu w 2001 r. W planie *eEurope + 2003: A Cooperative Effort to Implement the Information Society in Europe – Action Plan*[197] założono przyśpieszenie reform i pobudzenie modernizacji gospodarek państw kandydujących do Unii przez wykorzystanie narzędzi i technologii społeczeństwa informacyjnego. Jednym z głównych celów była też poprawa konkurencyjności i spójności społecznej, co poparły również kraje kandydujące w tym czasie do Unii Europejskiej[198].

21–22 czerwca 2002 r. w Sewilli odbył się szczyt Unii Europejskiej, podczas którego przyjęto plan rozwoju społeczeństwa informacyjnego do 2005 r.[199] W dokumencie *eEurope 2005: An Information Society for All – Action Plan* państwa członkowskie UE zobowiązały się do realizacji następujących zadań:

- rozwoju usług elektronicznych typu: e-learning, e-government, e-health;
- tworzenia dynamicznego środowiska do rozwoju gospodarki elektronicznej;
- zapewnienia powszechnego dostępu do Internetu szerokopasmowego;
- budowy systemu bezpieczeństwa infrastruktury informacyjnej.

W dokumencie Komisji Europejskiej z 2005 r. *i2010 – European Information Society for Growth and Employment* uznano, że wiedza i innowacje są motorem zrównoważonego wzrostu. Stwierdzono konieczność zbudowania integracyjnego społeczeństwa informacyjnego na fundamencie technologii informacyjnych i komunikacyjnych wykorzystywanych w administracji publicznej, małych i średnich podmiotach gospodarczych. Komisja Europejska określiła trzy priorytety polityki w zakresie budowy społeczeństwa informacyjnego: realizacja idei europejskiej przestrzeni informacyjnej promującej otwarty, konkurencyjny rynek, wspieranie

innowacji i inwestycji w technologie ICT w celu promowania rozwoju oraz wzrostu zatrudnienia oraz stworzenie europejskiego społeczeństwa informacyjnego. W komunikacie do programu podkreślono szybki postęp technologicznych, a technologie ICT są coraz powszechniej stosowane. W dziedzinie sieci komunikacyjnych, mediów, usług i urządzeń zachodzi konwergencja cyfrowa, dzięki coraz lepszym sieciom i technikom kompresji tworzą się nowe, szybsze kanały dystrybucji. Uznano, że jeżeli Unia Europejska ma w pełni wykorzystać swój potencjał gospodarczy, konieczne jest przyjęcie proaktywnego stanowiska politycznego stymulującego pozytywne trendy na rynku i wspierającego budowę społeczeństwa wiedzy, chroniącego konsumentów oraz zmierzającego do budowy bezpiecznego europejskiego społeczeństwa informacyjnego.

W komunikacie stwierdzono, że budując jednolitą przestrzeń informacyjną, konieczne jest odniesienie się do czterech głównych wyzwań związanych z konwergencją cyfrową: szybkości (dostępu do szybkich usług szerokopasmowych ułatwiających dostęp do zawartości multimedialnej, czyli np. wideo w wysokiej rozdzielczości), zawartości multimedialnej (poprawa sytuacji ekonomicznej i prawnej sprzyjającej powstawaniu nowych usług i zawartości online), interoperacyjności (ulepszenie urządzeń i platform oraz stworzenie usług umożliwiających komunikowanie się między różnymi platformami) oraz bezpieczeństwa (lepsze zabezpieczenie przed awariami technologicznymi, oszustwami i szkodliwą zawartością).

W komunikacie Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 2007 r. *W kierunku ogólnej strategii zwalczania cyberprzestępczości*[200] termin „cyberprzestępczość" został zdefiniowany jako czyny zabronione dokonane za pomocą lub skierowane przeciwko sieci łączności elektronicznej i systemom informatycznym.

Jedną z flagowych inicjatyw *Strategii Europa 2020* na rzecz zatrudnienia i wzrostu gospodarczego jest Europejska Agenda Cyfrowa, mająca na celu optymalizację korzyści płynących z technologii cyfrowych. Program zaczęto realizować w maju 2010 r.

Komisja Europejska przedstawiła propozycje regulacyjne w sprawie stworzenia jednolitego europejskiego rynku usług telekomunikacyjnych oraz wzmocnienia cyfrowych połączeń w Europie. Unia podjęła działania mające na celu zapewnienie otwartego dostępu do Internetu, zniesienia opłat roamingowych i lepszą ochronę konsumentów.

Przyszłe plany UE opisano w *Ramach polityki UE w zakresie cyberobrony* przyjętych w listopadzie 2014 r., w których określono pięć priorytetów w zakresie cyberobrony w kontekście WPBiO. Głównym celem jest wspieranie współpracy na szczeblach politycznym, technicznym i prawnym między państwami członkowskimi. Ważny jest także fragment, który podkreśla, że UE wyraża silną wolę „dalszej współpracy z NATO w zakresie cyberobrony”[201]. W przyszłości UE może wykorzystywać zasoby oraz potencjał NATO, tak jak to uczyniła, przejmując operacje wojskowe sojuszu na Bałkanach lub współpracując z NATO przy projektach dotyczących zwalczania piractwa oraz przeciwdziałając procederowi handlu ludźmi.

Globalna strategia UE na rzecz polityki zagranicznej i bezpieczeństwa została przyjęta przez Radę Europejską 28 czerwca 2016 r.[202] Określa wspólne interesy UE i państw członkowskich. Opiera się na następujących celach: bezpieczeństwie obywateli i terytorium, dobrobycie, demokracji, ładzie światowym, które mają doprowadzić do stworzenia wiarygodnej, reaktywnej i spójnej Unii Europejskiej. Zasady, którymi zaczęła kierować się Unia Europejska, to jedność, współdziałanie z innymi, odpowiedzialność, pogłębianie partnerstw zewnętrznych.

Aktualna strategia z 2016 r. identyfikuje pięć priorytetów, którymi są:

- bezpieczeństwo Unii, które ma polegać na intensyfikacji działań w zakresie obronności, bezpieczeństwa cybernetycznego, zwalczania terroryzmu oraz energii i strategicznej komunikacji;
- sąsiedztwo i odporność, którą zdefiniowano jako zdolność państw i społeczeństw do reformowania się, a tym samym do zwalczania różnych kryzysów, dzięki czemu będzie można

inwestować w odporność państw i społeczeństw leżących na wschód i południe od UE;
- zintegrowane podejście do sytuacji konfliktowych (wojna i kryzys), które będzie polegać na bezzwłocznym reagowaniu, działaniu, zapobieganiu oraz inwestowaniu w stabilizację;
- wspieranie stabilnych porządków regionalnych opartych na współpracy na całym świecie (regiony jako kluczowa przestrzeń ładu);
- skuteczne globalne rządzenie w XXI w., czyli działania na rzecz światowego ładu opartego na prawie międzynarodowym, zapewniające poszanowanie praw człowieka, zrównoważony rozwój oraz trwały dostęp do globalnych wspólnych dóbr[203].

Międzynarodowa współpraca w cyberprzestrzeni podkreśla zaangażowanie UE we wspieranie rozwoju budowania zaufania w cyberbezpieczeństwie, aby zwiększyć przejrzystość i zmniejszyć ryzyko nieporozumień, w zachowanie państwa polegające na promowaniu ustanawiania międzynarodowych norm w tej dziedzinie i wzywaniu Komisji oraz wysokiego przedstawiciela, zgodnie z odpowiednimi procedurami do promowania:
- konwencji budapeszteńskiej jako wzoru do opracowywania krajowej cyberprzestępczości,
- ustawodawstwa i podstawy międzynarodowej współpracy w tej dziedzinie,
- szacunku podstawowych praw w cyberprzestrzeni,
- pełnego wykorzystania wszystkich dostępnych międzynarodowych narzędzi współpracy służących rozwojowi walki z cyberprzestępczością, powiązanych ze współpracą policyjną i sądową w krajach trzecich, w których dochodzi do cyberprzestępczości,
- poszukiwania wiedzy specjalistycznej państw członkowskich w dziedzinie cyberprzestrzeni i ich doświadczeń w ramach stosunków dwustronnych[204].

We wrześniu 2017 r. Komisja Europejska rozpoczęła przegląd europejskiej strategii bezpieczeństwa cybernetycznego z 2013 r.,

wydając dokument roboczy przedstawiający jej ocenę[205]. Zgodnie z nim strategia ta była tylko częściowo skuteczna z powodu niewystarczających zasobów i ograniczonego zaangażowania kluczowych podmiotów. Ponadto od tamtej pory możliwości i zagrożenia w cyberprzestrzeni znacznie się rozwinęły. Czynniki te uzasadniły więc podjęcie ważnego kroku, tj. odnowienie strategii cyberbezpieczeństwa[206]. Sytuacja ta się zmieniła za sprawą wprowadzenia dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych (dyrektywa NIS). Akt ten formalnie stworzył sieć zespołów reagowania państw członkowskich na incydenty komputerowe (CSIRT), a sekretariat tej sieci zapewnia ENISA.

13 września 2017 r. Jean-Claude Juncker[207] powiedział: „W ostatnich trzech latach poczyniliśmy postępy w zapewnianiu Europejczykom bezpieczeństwa w sieci. Jednak Europa nadal nie jest właściwie przygotowana na cyberataki, dlatego Komisja przyjęła pakiet cyberbezpieczeństwa”[208]. Opiera się on na istniejących instrumentach i przedstawia nowe inicjatywy mające na celu dalszą poprawę odporności i reakcji cybernetycznej UE. W dokumencie tym po raz pierwszy wskazano potrzebę „utrzymania i rozwoju przez UE podstawowych zdolności do zapewnienia bezpieczeństwa gospodarki cyfrowej, społeczeństwa i demokracji”[209]. Celem polityki UE stało się zmniejszenie fragmentaryzacji rynku, a także rozwinięcie zdolności gospodarczych i poprawa działań wobec incydentów cybernetycznych. Konkretne działania polityczne nastąpiły w 2017 r. W tym kontekście należy wymienić działania unijne dotyczące partnerstwa publiczno-prywatnego na rzecz badań i innowacji. W ramach tej polityki stwierdzono potrzebę wprowadzenia nowego europejskiego systemu certyfikacji, który zagwarantuje, że produkty i usługi w świecie cyfrowym będą bezpieczne w użyciu.

Aby wyposażyć UE we właściwe narzędzia do walki z atakami cybernetycznymi, Komisja Europejska i Wysoki Przedstawiciel zaproponowali szeroki wachlarz środków mających na celu wzmocnienie bezpieczeństwa cybernetycznego. W tym celu wprowadzono zaktualizowaną strategię, której celem jest usprawnienie wspólnego podejścia państw członkowskich do

zjawiska cyberzagrożeń. Dotychczas rola Agencji Bezpieczeństwa Sieci i Informacji polegała głównie na dostarczaniu wiedzy i doradztwa, bez działań operacyjnych w obszarze bezpieczeństwa cybernetycznego. Nowe regulacje w z 2017 r. odnoszą się przede wszystkim do wzmocnienia tej agencji, przekształcając ją w podmiot o silnej roli doradczej w kwestii opracowywania i realizacji działań w obszarze cyberbezpieczeństwa. Określono wytyczne dotyczące jej kolejnego mandatu, który rozpocznie się w 2020 r.[210] i zostanie dostosowany do nowych europejskich ram bezpieczeństwa cyfrowego.

Podstawą reformy były działania przewidziane w strategii cyberbezpieczeństwa oraz główny filar strategii – dyrektywa o bezpieczeństwie sieci i informacji (dyrektywa NIS)[211]. Poza tym przewiduje się:

- utworzenie Europejskiego Centrum Badań Naukowych i Kompetencji w dziedzinie Bezpieczeństwa Cybernetycznego (projekt pilotażowy został zrealizowany w 2018 r.). Współpracując z państwami członkowskimi, pomoże ono w opracowywaniu i wdrażaniu narzędzi oraz technologii koniecznych, aby sprostać stale zmieniającym się zagrożeniom, i zagwarantuje, że obrona będzie tak nowoczesna, jak broń, którą posługują się cyberprzestępcy. Centrum będzie uzupełniać działania na rzecz budowy potencjału w tej dziedzinie na poziomach unijnym i krajowym[212];
- opracowanie planu szybkiego reagowania państw członkowskich umożliwiającego natychmiastową, skuteczną i skoordynowaną reakcję w przypadkach wystąpienia ataków cybernetycznych na dużą skalę. Ponadto wzywa się państwa członkowskie i instytucje UE do ustanowienia ram reagowania w sytuacji kryzysu cybernetycznego tak, aby można było ten[213] plan wprowadzić w życie. Będzie on poddawany regularnym testom w ramach ćwiczeń dotyczących zarządzania w sytuacji kryzysu cybernetycznego lub innej sytuacji kryzysowej;
- większą solidarność – w przyszłości można rozważyć możliwość utworzenia nowego funduszu pomocy w cybernetycznych

sytuacjach kryzysowych dla tych państw członkowskich, które odpowiedzialnie wdrożą wszystkie środki cyberbezpieczeństwa wymagane na podstawie prawa UE. Fundusz mógłby służyć zapewnianiu wsparcia państwom członkowskim w sytuacjach nadzwyczajnych, podobnie jak Unijny Mechanizm Ochrony Ludności jest wykorzystywany do pomocy w przypadku pożarów lub klęsk żywiołowych;

- wzmocnienie zdolności w zakresie obrony cybernetycznej – państwa członkowskie zachęca się do włączenia cyberobrony w ramy stałej współpracy strukturalnej (PESCO) i Europejskiego Funduszu Obrony, aby wspierać projekty dotyczące cyberobrony. Można też poszerzyć cyberobronę o zakres działania Europejskiego Centrum Badań Naukowych i Kompetencji w dziedzinie Bezpieczeństwa Cybernetycznego. Aby rozwiązać problem niedoboru wykwalifikowanej kadry w tym zakresie, w 2018 r. UE stworzyła platformę szkoleń i edukacji w dziedzinie cyberobrony. UE i NATO wspierają współpracę na rzecz badań naukowych i innowacji w dziedzinie obrony cybernetycznej. Współpraca z NATO zostanie zacieśniona przez udział w równoległych i skoordynowanych ćwiczeniach;
- pogłębienie współpracy międzynarodowej – UE wzmocni swoją zdolność reagowania na cyberataki, wprowadzając ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne wspierające strategiczne ramy zapobiegania konfliktom i stabilizacji w cyberprzestrzeni. Zostanie to połączone z wysiłkami na rzecz budowania nowych zdolności służących wspieraniu państw trzecich w walce z zagrożeniami cybernetycznymi[214].

Ważnym aktem prawnym jest rozporządzenie w sprawie ochrony danych (GDPR, inaczej RODO)[215], które wprowadziło zbiór spójnych i jednolitych regulacji dla wszystkich przedsiębiorstw działających w UE, które przetwarzają dane osobowe obywateli UE. Celem tego rozporządzenia jest ochrona praw jednostki w związku z przetwarzaniem danych osobowych. Zapisy określają prawo dostępu do informacji, regulują gromadzenie informacji,

przetwarzanie i przekazywanie danych między podmiotami publicznymi oraz dają obywatelom prawo do „bycia zapomnianym”, co wymaga od przedsiębiorstw usunięcia pewnych danych osobowych na wniosek obywatela. Dyrektywa NIS pozwala na zróżnicowanie działań ze względu na państwo, podczas gdy rozporządzenie GDPR oznacza to samo prawo dla każdego państwa. Dyrektywa NIS ma zastosowanie wyłącznie do operatorów krytycznych, a rozporządzenie GDPR – do każdego, kto ma do czynienia z danymi osobowymi. Inną różnicą jest to, że GDPR potencjalnie narzuca wysokie grzywny za naruszenie ochrony danych osobowych, jednak jak dotąd grzywny z tytułu bezpieczeństwa sieci i informacji wydają się mniejsze[216].

9 kwietnia 2019 r. Rada przyjęła rozporządzenie zwane aktem o cyberbezpieczeństwie[217], które ustanowiło system certyfikacji na poziomie unijnym oraz zmodernizowaną agencję UE ds. cyberbezpieczeństwa zastępującą ENISA. Ustanowiła też przepisy, które pozwalają nakładać unijne ukierunkowane środki ograniczające, by zapobiegać cyberatakom stanowiącym zewnętrzne zagrożenie Unii lub jej państw członkowskich i reagować na nie. Dzięki tej decyzji UE po raz pierwszy będzie mogła nakładać sankcje na osoby lub podmioty, które:

- odpowiadają za dokonanie lub próby dokonania cyberataków,
- zapewniają w tym celu wsparcie finansowe, techniczne lub materialne,
- angażują się w te działania w inny sposób.

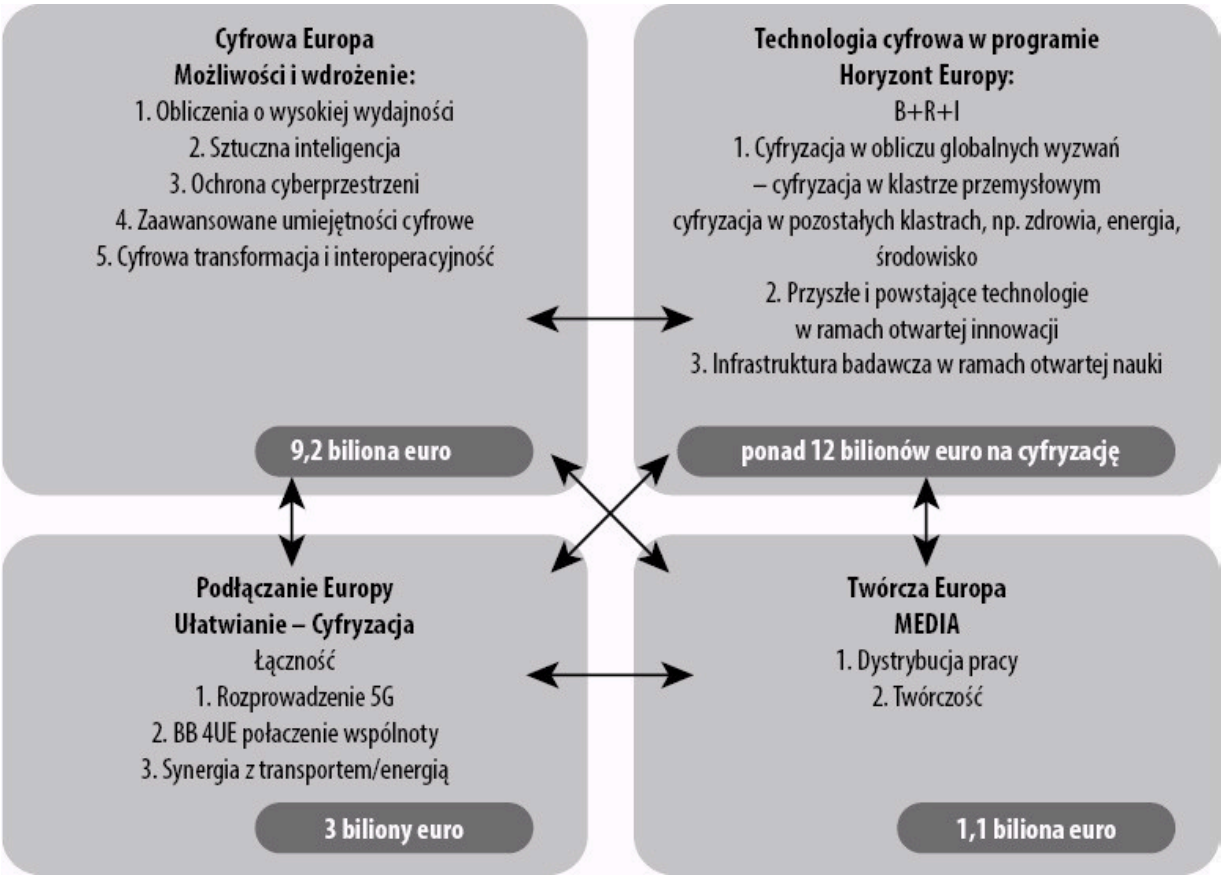
W ramach tej samej reformy UE wprowadziła także przepisy, na których mocy powstało Europejskie Centrum Badań Naukowych i Kompetencji w dziedzinie Cyberbezpieczeństwa wspierane przez sieć krajowych ośrodków koordynacyjnych. Struktury te pomogą zabezpieczyć jednolity rynek cyfrowy (art. 114 TFUE) i zwiększyć autonomię UE w dziedzinie cyberbezpieczeństwa. Ponadto UE może wymierzać sankcje wobec osób lub podmiotów unijnych, a także przeciwko państwom spoza UE lub organizacjom międzynarodowym, jeżeli uzna to za konieczne do osiągnięcia celów wspólnej polityki zagranicznej i bezpieczeństwa.

Jednocześnie UE pracuje nad środkami międzysektorowymi, które pomogą eliminować cyberzagrożenia w kilku obszarach naraz. Przykładem są:

- walka z przestępczością zorganizowaną, w tym obszarze cyberprzestępczość została uznana za jeden z 10 priorytetów na lata 2018–2021,
- wspólna polityka zagraniczna i bezpieczeństwa, realizacja jej celów zależy również od udanego zapobiegania cyberatakom,
- cyberobrona – UE zaktualizowała przepisy cyberobronne, uwzględniając ewoluujące wyzwania w zakresie bezpieczeństwa[218].

Najnowszym posunięciem w polityce cyberbezpieczeństwa jest wydanie *Białej Księgi* z 2020 r. dotyczącej sztucznej inteligencji (AI) i cyfryzacji, która ma stanowić klucz do zwalczenia cyberterroryzmu i osiągnięcia ładu klimatycznego przez doskonalenie AI[219]. To element konieczny pozwalający na utrzymanie jednolitego rynku UE przez badania naukowe, innowacje i wdrożenie do grudnia 2020 r. skoordynowanego planu działań w ramach programów *Cyfrowa Europa* oraz *Horyzont Europa* na lata 2021–2027.

Opracowanie planu szybkiego reagowania państw członkowskich umożliwi natychmiastową, skuteczną i skoordynowaną reakcję w przypadkach wystąpienia ataków cybernetycznych na dużą skalę. Pogłębienie współpracy międzynarodowej UE ma celu wzmocnienie zdolności reagowania na cyberataki, wprowadzając ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne wspierające strategiczne ramy zapobiegania konfliktom i stabilizacji w cyberprzestrzeni. Zostanie to połączone z wysiłkami na rzecz budowania nowych zdolności służących wspieraniu państw trzecich w walce z zagrożeniami cybernetycznymi[220].



RYSUNEK 2.1 Programy Cyfrowa Europa oraz Horyzont Europa na lata 2021–2027
Źródło: europa.eu.(https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52018PC0434) oraz https://www.swisscore.org/Documents/RI_Seminar_2019_Annalisa_Bogliolo.pdf (dostęp: 30.06.2020).

* * *

Polityka i strategia określają byt i rozwój państwa. Truizm ten pozwala na spostrzeżenie, że dzieje się to w związku z umiejętnością jego zapewnienia w stosunku do wartości, potrzeb, interesów, celów, które warunkują realizację polityki i strategii państwa w perspektywie krótko-, średnio- i długoterminowej. Dzięki tym umiejętnościom lub ich brakowi państwo generuje w czasie i przestrzeni swoją siłę, potęgę, wpływ, który wywiera na pozostałe podmioty – państwa i ich organizacje, społeczności i społeczeństwo, naród. Polityka i strategia są przy tym warunkowane przez

wyzwania, zagrożenia, szanse dla bytu i rozwoju podmiotu, czyli jego wizji, misji i celów, które podejmuje bądź realizuje.

Kolejnym truizmem jest zatem twierdzenie, że umiejętne połączenie polityki i strategii warunkuje pomyślność działań w każdej ze sfer aktywności państwa: społeczno-kulturowej, ekonomicznej i bezpieczeństwa. Polityka i strategia są przy tym zwykle zmienne, dynamiczne i stale aktualizowane (najczęściej w ramach tzw. przeglądu strategicznego, który periodycznie weryfikuje założenia strategii[221]). Związek między polityką a strategią, czyli długookresową koncepcją działania politycznego oraz praktycznymi metodami ich realizacji w czasie i przestrzeni z wykorzystaniem dostępnych, potencjalnych oraz kreowanych sił i środków jest przy tym podstawowym czynnikiem kształtowania bytu i rozwoju państwa.

Rola przeglądu strategicznego jako narzędzia analizy strategii w wymiarze wewnętrznym i zewnętrznym, rozpoznania silnych i słabych stron, weryfikowania potencjału (rzeczywistych możliwości), formułowania podstaw przyszłych działań strategicznych (politycznych, ekonomicznych, społeczno-kulturowych, militarnych) jest przy tym niezwykle istotna. Pozwala bowiem na korektę polityki i strategii, czyniąc z nich dwa wzajemnie uzupełniające się elementy. Dzięki temu obrany kierunek polityki i strategii, wyrażany w formie celów będących pochodną interesów, potrzeb i wartości społeczeństwa, jest stale utrzymywany, choć mogą się zmieniać formy i sposoby jego realizacji. Ponadto wykorzystanie przeglądu strategicznego jako narzędzia weryfikacji założeń, sposobów realizacji polityki i strategii pozwala dokonywać stałej analizy strategii w wymiarze zewnętrznym oraz wewnętrznym podmiotu, rozpoznania jego silnych i słabych stron, weryfikacji potencjału (rzeczywistych możliwości) oraz weryfikacji podstaw przyszłych działań strategicznych.

Odniesienie do czynników kulturowych można coraz częściej znaleźć w doktrynach i strategiach bezpieczeństwa narodowego i obronności[222]. W ten sposób został poszerzony przedmiotowy katalog bezpieczeństwa o nowy wymiar kulturowy, co wcale nie

znaczy, że uprzednio kulturowe aspekty bezpieczeństwa nie były uświadamiane i omawiane, a problem bezpieczeństwa kulturowego, choć inaczej nazywany i niepoddawany konceptualizacji, towarzyszył wojnom, podbojom, a także mniej dramatycznym spotkaniom kulturowym. Przegląd strategiczny jako narzędzie weryfikacji założeń, sposobów realizacji polityki i strategii pozwala dokonywać stałej analizy strategii w wymiarze zewnętrznym oraz wewnętrznym podmiotu, rozpoznania jego silnych i słabych stron, weryfikacji potencjału (rzeczywistych możliwości) i weryfikacji podstaw przyszłych działań strategicznych.

Odnosząc się do polityki i strategii państwa realizowanej w wymiarze zewnętrznym, będzie ona zasadniczo efektem wzajemnych interakcji między podmiotem a otoczeniem w kontekście istniejących lub potencjalnych szans, wyzwań oraz zagrożeń. Sprawia to, że państwa w sytuacji narastającej kompleksowości interakcji będącej pochodną procesów globalizacji w coraz większym stopniu cedują swoją politykę oraz realizację strategii na tworzone przez siebie wspólnoty międzynarodowe. W efekcie następuje przenikanie polityki wewnętrznej z zewnętrzną, a także korelacja między strategią wspólnotową a państwową. Na tym tle dochodzi także do korelacji celów, interesów, potrzeb, a w konsekwencji upowszechniania wspólnych wartości między państwami, które tworzą instytucje i organizacje, a także wspólnoty międzynarodowe.

Mówiąc o znaczeniu polityki i strategii państwa w kontekście ich formułowania, należy przede wszystkim wskazać na kategorie poznania naukowego, które określają wzajemny związek. Są to wymienione wcześniej wyzwania, zagrożenia, szanse, spełniające funkcje kryteriów oceny istoty, zakresu, charakteru polityki i strategii państwa, w wymiarze zarówno zewnętrznym, jak i wewnętrznym. Kryteria te w kontekście polityki i strategii państwa nie występują przy tym samoistnie, lecz są zwykle odnoszone do wizji, misji oraz celu działań podmiotu. Należy przy tym podkreślić, że wizja podmiotu wyraża konceptualną gotowość do sprostania wyzwaniom, zagrożeniom, szansom, zwykle określającym jego działania na rzecz zapewnienia bytu i rozwoju w średnio- i długoterminowej perspektywie. Misja podmiotu określa sposób jego

bieżącego działania na rzecz zapewnienia bytu i rozwoju w stosunku do istniejących (rozpoznanych) wyzwań, zagrożeń i szans. Cele podmiotu wyznaczają natomiast kierunek działań (realizowanych bądź podejmowanych) w stosunku do istniejących (rozpoznanych) oraz prognozowanych wyzwań, zagrożeń i szans[223].

W związku z tym należy zgodzić się z Jarosławem Gryzem, że rzeczywistą potrzebą państwa jest podjęcie działań, które przyczyniłyby się do stworzenia systemu, wypracowywania modyfikacji, implementacji strategii i innych pochodnych dokumentów. Taka konkluzja niesie ze sobą wiele implikacji głównie natury organizacyjnej.

3

UWARUNKOWANIA CYBERBEZPIECZEŃSTWA UNII EUROPEJSKIEJ

Traktując kompleksowo pojmowanie bezpieczeństwa, zwraca się obecnie uwagę na militarne i pozamilitarne aspekty tej problematyki oraz jej personalne i strukturalne konteksty. Jak już wcześniej wspomniano, bezpieczeństwo jest potrzebą podmiotową, może dotyczyć zarówno jednostek, jak i dużych grup społecznych, włączając w to struktury organizacyjne (instytucje) je reprezentujące. Jednym z podstawowych zadań każdego państwa jest zapewnienie bezpieczeństwa, które jest konieczne do stworzenia określonych warunków do działalności i rozwoju społeczeństwa. Należy więc uwzględnić aspekty polityczne, ekonomiczne, społeczne, militarne, gdyż bezpieczeństwo jest określoną wartością społeczną, nie tylko cywilizacyjną, kulturową, polityczną, ekonomiczną i ekologiczną, ale także wartością egzystencjalną, moralną i duchową.

W rzeczywistości międzynarodowej brakuje czynnika, który określałby reguły wzajemnego zachowania się państw, zapobiegał konfliktom między nimi i bronił przed napaścią. Założenia charakterystyczne dla realistów w gruncie rzeczy sprowadzają się do wąskiego rozumienia bezpieczeństwa opartego na atrybutach siły militarnej i poszukiwania równowagi sił w mającej cechy anarchiczne sferze stosunków międzynarodowych.

Polityka bezpieczeństwa zależy od wielu czynników i uwarunkowań, które mieszczą się w teorii bezpieczeństwa. Z reguły dzieli się ją na wewnętrzną i zewnętrzną, obiektywną i subiektywną. Duże znaczenie ma również struktura polityki bezpieczeństwa, zwłaszcza gdy mamy na uwadze wszystkie trzy obszary – narodowy, regionalny i globalny. Bezpieczeństwo globalne i lokalne uwarunkowane jest wieloma czynnikami, w tym politycznymi. Polityka wewnętrzna i zewnętrzna prowadzone przez dany podmiot wpływają na poczucie bezpieczeństwa obywateli i warunkują jego miejsce w rzeczywistości międzynarodowej. Bezpośrednie zagrożenie jest związane z możliwością wystąpienia wojny, ze stanem pozostawania w stanie wojny lub oficjalnym prowadzeniem konfliktu militarnego. Na potencjalne zagrożenia i wyzwania dotyczące kształtowania bezpieczeństwa danego państwa mają wpływ jego relacje z sąsiadami. Również kryzys polityczny, gospodarczy, społeczny czy kulturowy może wpływać na sytuację międzynarodową kraju.

Po zakończeniu zimnej wojny i rozpadzie układu dwubiegunowego znacznie spadła skala, zakres i natężenie tradycyjnych zagrożeń militarnych (odnosiło się to przede wszystkim do obszaru transatlantyckiego). Zmniejszenie ryzyka wybuchu wojny ogólnoświatowej nie przełożyło się natomiast na złagodzenie konfliktów regionalnych czy lokalnych – te się nawet zaostrzyły. Jednocześnie rozwinęły się lub uzyskały nowe formy zagrożenia asymetryczne, czego najlepszym przykładem są dzisiejsze ataki terrorystyczne czy cyberterrorystyczne zarówno w UE, jak i poza jej obszarem. Kolejnym dowodem zagrożenia asymetrycznego w

ostatnich latach był tzw. kryzys migracyjny UE. Definiowanie zagrożeń asymetrycznych w ujęciu wojskowym opiera się na niekonwencjonalnych sposobach działań przeciwnika, wynikających z nieproporcjonalności w potencjałach wojskowych.

Ujęcie politologiczne z kolei wiąże zagrożenia asymetryczne wyłącznie z aktywnością podmiotów pozapaństwowych, trans- lub subnarodowych. W takiej sytuacji odmienność metod działania i sposobów prowadzenia konfliktu oraz dysproporcja potencjałów (militarnych) stron układu wynika z faktu, że podmiot zagrożony (państwo) i stanowiący zagrożenie należą do różnych kategorii uczestników stosunków międzynarodowych. Takie ujęcie zagrożeń asymetrycznych umożliwia podkreślenie specyfiki gróźb ze strony podmiotów pozapaństwowych oraz pozwala na bardziej jednoznaczne odróżnienie ich od tradycyjnych niebezpieczeństw stanowionych przez państwa.

Zgodnie ze stanowiskiem szerzej definiującym zakres podmiotowy zagrożeń asymetrycznych tego typu zagrożeniem jest każdy podmiot stosujący metody uznawane w danych okolicznościach za asymetryczne. Oznacza to, że zakres podmiotowy zagrożeń asymetrycznych może być zróżnicowany w zależności od tego, jaki podmiot był przedmiotem ataku. Dla określonego państwa zagrożeniem asymetrycznym może być zarówno inne państwo, jak i podmiot pozapaństwowy. Wśród zagrożeń asymetrycznych w szerokim ujęciu wymienia się wiele zjawisk, przy czym kryterium wyodrębniania poszczególnych grup stanowi nie rodzaj stwarzającego zagrożenie, lecz specyficzny charakter użytych przez niego środków lub metod działania. W węższym ujęciu podmiotowym zagrożeń asymetrycznych pozapaństwowych uczestników stosunków międzynarodowych następuje redukcja poziomu relatywizacji tego pojęcia, czyli zyskuje ono bardziej uniwersalny charakter (praktycznie niezależnie od posiadanego przez dane państwo potencjału militarnego i pozamilitarnego). Wśród tak rozumianych zagrożeń asymetrycznych wyróżnia się najczęściej cztery główne rodzaje: terroryzm międzynarodowy, transnarodowa przestępczość zorganizowana, użycie broni masowego rażenia przez podmioty pozapaństwowe oraz cyberprzestępczość.

Miało na to wpływ wiele czynników, które się nawzajem wzmacniały, np. przemiany ładu międzynarodowego, nowe podziały, konflikty i in. Zagrożenia asymetryczne stanowią niejednorodną grupę zjawisk. Istotne różnice występują nie tylko między ich głównymi rodzajami, ale także między poszczególnymi podmiotami należącymi do tego samego typu zagrożeń asymetrycznych. Można jednak wskazać pewne cechy wspólne podmiotów będących zagrożeniami asymetrycznymi. Natężenie ich występowania różni się w zależności od typu zagrożenia oraz konkretnego podmiotu stanowiącego jego źródło. Te wyróżniki są ściśle ze sobą związane, nierzadko wynikają jedne z drugich i wzajemnie się wzmacniają. One też w największym stopniu decydują o odmienności zagrożeń asymetrycznych od tradycyjnych gróźb dla bezpieczeństwa państw. Czynnikami najmocniej oddziałującymi są pozapaństwowy charakter podmiotów je stanowiących oraz łącząca się z nim ich transnarodowość i terytorialność, czyli brak jasno określonego obszaru występowania czy też definiowanego geograficznie terytorium, nad którym podmioty te sprawowałyby wyłączną zwierzchność i egzekwowały suwerenność.

Zagrożenia ze strony podmiotów pozapaństwowych określane są jako quasi-militarne. Ważnym determinantem w kontekście polityki przeciwdziałania takim zjawiskom jest ich niska podatność na odstraszanie oraz politykę zwalczania i zapobiegania. To konsekwencja aterytorialności takich podmiotów[224].

Nowy terroryzm, jakim stał się cyberterroryzm, jest wynikiem ery informatyzacji. Informacja, będąca obiektem badań oraz dociekań naukowych i praktycznych, jest przedmiotem zainteresowania wielu specjalistów z różnych dziedzin.

Podstawową cechą cyberterroryzmu jest sieciowość, co oznacza nie tylko odejście od klasycznej struktury hierarchicznej organizacji, ale także brak stałej lokalizacji, bezterytorialność. Działania i koordynacja elementów systemu nie są formalnie skodyfikowane przez relacje hierarchiczne, lecz wyłaniają się i zmieniają w zależności od konkretnego zadania. Kolejną cechą takich organizacji jest to, że więzy zewnętrzne i wewnętrzne nie są skutkiem decyzji biurokratycznych, lecz efektem wspólnych norm, wartości, interesów i wzajemnego zaufania[225].

Należy stwierdzić, że przyczyną powstania tej polityki był również brak istnienia krajowych planów strategicznych dotyczących cyberbezpieczeństwa, dlatego polityka Unii Europejskiej w tym zakresie jest nie tylko odpowiedzią, ale także efektem działań prowadzonych na poziomach regionalnym i państwowym. Przyczyną jej powstania był również brak odpowiednich mechanizmów i regulacji, dlatego mamy do czynienia z tzw. procesem instytucjonalizacji.

W niniejszym rozdziale zostaną wskazane i omówione uwarunkowania zewnętrzne i wewnętrzne, które przyczyniły się do powstania polityki ochrony cyberbezpieczeństwa. Skupiono się w szczególności na uwarunkowaniach UE na rzecz włączenia bezpieczeństwa cybernetycznego do jej polityki zagranicznej i zaangażowania państw trzecich w tym obszarze.

W dotychczasowej działalności UE skupiała się na integracji gospodarczej, jednak obawy związane z brakiem bezpieczeństwa cybernetycznego w coraz większym stopniu prowadziły do inicjatyw na rzecz wzmocnienia bezpieczeństwa w tym zakresie za pomocą norm, regulacji i rozwoju kapitału ludzkiego na szczeblu europejskim. Kształtowanie polityki bezpieczeństwa cybernetycznego na poziomie UE stanowi wyzwanie ze względu na różnorodność interesów państw członkowskich oraz ograniczony mandat UE w przypadku obszaru dotyczącego bezpieczeństwa narodowego.

3.1
ISTOTA I ZAKRES CYBERTERRORYZMU JAKO ZAGROŻENIA W XXI W.

Bezpieczeństwo jest najczęściej określane i definiowane w kontekście wyzwań i zagrożeń dla danego podmiotu. Wyzwanie różni się tym od zagrożenia, że zagrożenie jest sytuacją, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia. Oznacza ono wysokie ryzyko powstania konfliktu lub wystąpienie bezpośredniego prawdopodobieństwa jego powstania. W przypadku wyzwań natomiast istnieje tylko przesłanka powstania konfliktu. Wyzwania i zagrożenia bezpieczeństwa to terminy często utożsamiane. Istotna różnica polega na tym, że wyzwania w przeciwieństwie do zagrożeń oznaczają zjawiska nowe bądź na nowo odkrywane i nie wiążą się bezpośrednio z wystąpieniem ryzyka konfliktu zbrojnego, stanowią jedynie jego przesłankę. Jednak wyzwanie może przekształcić się w zagrożenie.

Przyczyny zagrożeń bezpieczeństwa są zróżnicowane i podlegają ewolucji podążającej za rozwojem stosunków międzynarodowych, zmianą interesów państw odgrywających kluczową rolę na arenie międzynarodowej, znaczeniem organizacji międzynarodowych oraz przeobrażeniami, jakie zachodzą w technice i technologii wojskowej oraz cywilnej. Do współczesnych wyzwań i zagrożeń zalicza się:

- niekontrolowaną proliferację broni masowego rażenia oraz środków jej przenoszenia (Korea Północna),

- COVID-19,
- międzynarodowy terroryzm fundamentalistów islamskich,
- transgraniczną przestępczość zorganizowaną,
- regionalne i lokalne konflikty zbrojne (uchodźcy),
- problemy państw „upadłych",
- pogłębiające się dysproporcje rozwojowe między państwami bogatymi a biednymi (emigranci ekonomiczni),
- wzrastające zapotrzebowanie na surowce energetyczne,

zagrożenia w nowym środowisku bezpieczeństwa – cyberprzestrzeni[226].

„Zagrożenie" to termin pochodzący od słowa „grozić" – stwarzać stan niebezpieczeństwa, być niebezpiecznym, zagrażać. „Groźba" natomiast oznacza zapowiedź niebezpieczeństwa, kary, zemsty, to pogróżka[227]. Rzeczownik ten pochodzi od słowa „zagrozić", które oznacza sytuację lub stan, które komuś czymś zagrażają lub w których ktoś czuje się zagrożony bądź ktoś stwarza taką sytuację[228]. „Zagrożenie" definiowane jest także jako sytuacja będąca sygnałem czegoś, co może nastąpić, zwykle złego, niepożądanego lub niebezpiecznego[229]. Jego synonimami są takie pojęcia jak niebezpieczeństwo, groźba, ryzyko, niepewność, niepokój, niestabilność, obawa[230].

Termin „zagrożenie" odnoszący się do systemu informatycznego został zdefiniowany przez Krzysztofa Lidermana jako:

- potencjalne naruszenie zabezpieczenia systemu informatycznego,
- podatność, wada lub luka w strukturze fizycznej, organizacji, procedurach, personelu, zarządzaniu, administrowaniu, sprzęcie lub oprogramowaniu, która może być wykorzystana do spowodowania szkód w systemie informatycznym lub działalności człowieka[231].

Literatura przedmiotu jednoznacznie nie wskazuje, które zagrożenia będą stanowiły największe niebezpieczeństwo dla sieci komputerowych. Nie można również określić, które są najważniejsze. Za celowy należy zatem uznać ogólny podział zagrożeń na zewnętrzne i wewnętrzne.

Zagrożenia zewnętrzne mają miejsce, gdy może dojść do utraty, uszkodzenia danych, utraty możliwości obsługi systemu lub sieci informatycznej w wyniku celowego lub przypadkowego działania ze strony osób nieuprawnionych, działających z zewnątrz w stosunku do danego systemu informatycznego. Wśród tych zagrożeń wymienia się m.in.:

- utratę lub zniekształcenie danych przez wadliwą pracę urządzeń czy oprogramowania (w tym celowo wprowadzonych wirusów) – ataki w cyberprzestrzeni;
- zaniedbanie lub zaniechanie działań mających wpływ na sprawność techniczną użytkowanego sprzętu;
- zmiany w zdalnym sterowaniu sieciami (zmiana zabezpieczeń, konfiguracji, uprawnień dostępu), jak również brak możliwości zarządzania lub sterowania siecią lub systemem informatycznym[232].

Zagrożenia wewnętrzne występują, „gdy zachodzi lub zaszła możliwość utraty lub uszkodzenia danych, utrata możliwości obsługi sieci teleinformatycznej w wyniku celowego bądź przypadkowego działania ze strony osób nieuprawnionych działających w wewnętrznym otoczeniu sieci"[233]. Zagrożenia wewnętrzne mogą być skutkiem:

- utraty i uszkodzenia danych w wyniku celowego działania użytkowników;
- braku możliwości obsługi sieci informatycznej z powodu jego błędnej pracy,

- strat w wyniku nieautoryzowanego dostępu do informacji;
- zniszczenia danych spowodowanego błędami w oprogramowaniu systemowym, użytkowym lub wprowadzeniem oprogramowania złośliwego[234].

William J. Lynn III wymienia charakterystyczne cechy wyzwań i zagrożeń bezpieczeństwa w cyberprzestrzeni. Są to:
- asymetryczność – szczególna cecha rozumiana jako dysproporcja między technikami ataku a obrony, techniki ataku cechują się niskim poziomem zaawansowania (małe koszty), techniki obrony natomiast − skomplikowanym stopniem zaawansowania (duże koszty),
- szybkość i skrytość ataku – atak jest przeprowadzany bardzo szybko, a rozpoznanie atakującego może w ogóle nie być możliwe,
- otwarta natura cyberprzestrzeni – ze względu na dostępność i otwartość Internetu systemy cyberobrony pojawiły się z pewnym opóźnieniem w stosunku do cyberzagrożeń[235].

Cechami wspólnymi wszystkich cyberataków są:
- trudności ich wykrycia − atak można wykonać z innego państwa, za pomocą obcego komputera lub przeprowadzić z publicznego miejsca,
- wysoki stopień anonimowości cyberagresorów,
- duża siła rażenia,
- niezwykła łatwość przeprowadzenia ataków,
- niskie koszty przedsięwzięcia[236].

Znawcy tematu wyróżniają kluczową grupę osób przeprowadzających ataki w cyberprzestrzeni, do której zaliczają:
- hakerów atakujących komputery dla wyzwania, zdobycia pozycji lub uzyskania dostępu do systemu,
- szpiegów, którzy dążą do zdobycia informacji, aby wykorzystać ją w celach politycznych,
- terrorystów atakujących komputery, aby wzbudzić strach,
- agresorów wewnętrznych – pracowników firm, którzy dokonują ataków dla korzyści materialnych,
- zawodowych przestępców atakujących komputery dla osobistych korzyści materialnych,
- wandali, którzy dążą do wyrządzenia jak największych szkód,
- podglądaczy, którzy dążą do przejęcia ważnych informacji[237].

Zdaniem ekspertów nie można całkowicie wyeliminować prawdopodobieństwa wystąpienia czynników niebezpiecznych dla informacji. Można jedynie obniżać poziom zagrożenia, czyli minimalizować negatywne skutki w przypadku wystąpienia czynników niebezpiecznych. Wobec tego bezpieczeństwo informacyjne często określa się jako stan, w którym ryzyko wystąpienia zagrożeń związanych z prawidłowym funkcjonowaniem zasobów informacyjnych jest ograniczone do akceptowalnego poziomu[238].

Rozwój cywilizacji, technologii, społeczeństwa informacyjnego warunkuje powstanie wyzwań, które mogą przeobrazić się w zagrożenia. Piotr Bączek wymienia podstawowe zagrożenia informacyjne we współczesnym świecie, którymi są:
- nieuprawnione ujawnienia informacji,
- naruszenia przez władze praw obywatelskich,
- asymetria w międzynarodowej wymianie informacji,
- działalność grup świadomie manipulujących przekazem informacji,

- niekontrolowanie technologii bioinformatycznych,
- przestępstwa komputerowe,
- cyberterroryzm,
- walka informacyjna,
- zagrożenia asymetryczne,
- szpiegostwo[239].

Głównym zagrożeniem bezpieczeństwa informacyjnego jest brak aktualnej, prawdziwej, sprawdzonej informacji koniecznej do podejmowania decyzji. Równie niebezpieczny jest nadmiar informacji, których większość jest bezużyteczna i małej wartości. Prowadzi do chaosu informacyjnego spowodowanego brakiem właściwej organizacji i zarządzania informacją oraz stosowaniem technik manipulacyjnych. Adam Lepa uważa, że „poczucie chaosu w pewnych dziedzinach życia publicznego, np. polityce, gospodarce, prawodawstwie, w wiedzy o własnym społeczeństwie bywa następstwem działań manipulatorskich. Prowadzi do tego wyczerpujące bombardowanie psychiki człowieka wielością niezrozumiałych bodźców, a także przekazywanie sprzecznych ze sobą i nakładających się informacji”[240]. Specjaliści określają bezpieczeństwo informacyjne jako ochronę informacji przed przypadkowym lub świadomym ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania. Celem środków bezpieczeństwa jest zapewnienie poufności, integralności i dostępności informacji, czyli wyeliminowanie zagrożenia[241].

TABELA 3.1. Obszary specyficznych ograniczeń cyberprzestrzeni

Obszar	Charakterystyka
Prawo	• niejasne i niespójne • niejasna odpowiedzialność za czyny i wykroczenia • brak międzynarodowych (narodowych) kryteriów klasyfikacji i kwalifikacji • nieprecyzyjne określenia aktów kryminalnych i aktów zagrożeń bezpieczeństwa narodowego
Przestrzeń	• brak przestrzennych granic • brak politycznych granic • brak geograficznych granic • brak doraźnych granic
Zagrożenia	• prosta, ogólnie dostępna technologia • anonimowość sprawy • wielość form cyberataków • „efekt domina” jako skutek
Bezpieczeństwo	• brak szybkich i skutecznych rozwiązań zabezpieczających • mnogość obiektów zagrożeń (ataków) • wysokie koszty zabezpieczeń • zróżnicowana podatność obiektów • nieprzewidywalność źródeł zagrożeń • bardzo wysokie koszty

Źródło: P. Sienkiewicz, *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe WWSI” 2015, nr 13, t. 9, s. 98.

Do pierwszej grupy zagrożeń należą sabotaż i zagrożenia nieumyślne, które charakteryzuje występowanie szkody bez bezpośredniego materialnego lub informacyjnego zysku. Ta kategoria obejmuje awarie zasilania energetycznego, pożary, klęski żywiołowe, dezintegrację, a także inne fizyczne czynniki destrukcyjne. Przykładem dezintegracji lub destrukcji informatycznej mogą być wirusy komputerowe, bomby logiczne i konie trojańskie, a fizycznymi czynnikami destrukcyjnymi są m.in. ładunki wybuchowe niszczące aparaturę komputerową[242].

Analiza literatury wskazuje, że obecnie w cyberprzestrzeni stosuje się następujące rodzaje ataków:

- SYN flood[243],
- DoS (*Denial of Service*)[244],
- DDoS (*Distributed Denial of Service*)[245],
- DRDoS (*Distributed Reflection Denial of Service*)[246],
- Fork-bomba (*Fork Bomb*)[247].

Są to ataki, które nie umożliwiają intruzowi uzyskania dostępu do informacji w systemie, nie powodują też utraty i kradzieży danych. Skutkiem ich działania jest zablokowanie pracy sieci i usług, co ogranicza i uniemożliwia (na określony czas) funkcjonowanie organizacji i naraża ją na znaczne straty i koszty.

Drugą grupą zagrożeń jest infiltracja, czyli „działania osób nieupoważnionych, mające na celu przenikanie do różnych elementów systemu informatycznego lub sieci telekomunikacyjnej w celu zdobycia informacji za pomocą różnych sposobów i środków". Cechą charakterystyczną tej metody jest chęć zysku z posiadania zdobytych informacji. Infiltracja dzieli się na dwie kategorie: czynną i bierną. Infiltracja bierna polega na śledzeniu informacji w określonym miejscu jej obiegu. Najczęściej stosowanymi technikami są:

- „przechwytywanie elektromagnetyczne polegające bądź na uzyskaniu dostępu do połączeń między komputerem a terminalami, bądź do kierunkowej emisji promieniowania i na analizie sygnału odbitego od promieniującego urządzenia;
- dołączenie się do linii transmisji danych w sieciach telekomunikacyjnych lub przechwytywanie sygnałów przekazywanych drogą radiową;
- badanie i kopiowanie zasobów niezabezpieczonych (piractwo komputerowe)[248].

Rozwój społeczeństwa informacyjnego niesie nowe perspektywy, nowe rozwiązania, nowe technologie i nowe instytucje. Prowadzi to do pojawienia się nowych wyzwań i zagrożeń, które mogą wystąpić w sferze informacyjnej:

- terroryzm, jako wynik zmian w zakresie dostępu do nowych technik negatywnego oddziaływania i niszczenia (cyberterroryzm);
- konflikty o prawo do informacji, przetwarzania informacji, dystrybucji informacji,
- cyberprzestrzeń jako obszar konfliktu;
- informacja jako czynnik rozwarstwienia w gospodarce światowej;
- zjawisko „globalnej wioski" jako czynnik dezintegrujący tradycyjne struktury społeczne, powodujące erozje autorytetu władzy, pozbawiający obywateli tradycyjnej ochrony, którą roztaczało państwo;
- stale narastający rozwój zorganizowanej przestępczości, szczególnie przestępczości wykorzystującej cyberprzestrzeń i korzystającej z osiągnięć technologii;
- rosnąca liczba przestępstw bankowych, skarbowych, kryminalnych, których środowiskiem będzie przestrzeń cybernetyczna;
- informatyzacja i militaryzacja przestrzeni kosmicznej[249].

Cyberterroryzm stał się modnym pojęciem, jednak niewiele osób wie, czym on tak naprawdę jest. Wielu uważa, że to jedynie teoretyczne pojęcie, działanie, które prawdopodobnie nigdy nie będzie miało miejsca. Jednak nikt nie wie, co przyniesie przyszłość.

Powszechne wykorzystywanie technologii informatycznych jest niewątpliwie szczególnym atrybutem współczesności. Komputer i Internet to narzędzia, bez których nie potrafi dziś

normalnie funkcjonować ani administracja, ani gospodarka, ani obywatel. Dzięki informatyzacji zwiększył się dostęp do informacji, pojawiła się łatwość przetwarzania każdej informacji, zwiększyły się możliwości komunikacyjne, a cały świat staje się powoli globalną wioską. Zmiany cywilizacyjne, jakie nastąpiły w ostatnich latach, są ogromne i nieodwracalne, a ich skutki nie do końca jeszcze przewidywalne.

Zdefiniowanie cyberterroryzmu jako połączenia cyberprzestrzeni i terroryzmu oznacza, że taka aktywność wiąże się nie tylko z wrogim użyciem IT i działaniem w sferze wirtualnej, ale także cechuje się wszystkimi elementami konstytuującymi aktywność terrorystyczną[250]. Pojęcie to odnosi się do bezprawnych ataków i zagrożeń wobec komputerów, sieci i informacji przechowywanych w nich, których celem jest zastraszenie lub zmuszenie rządu albo jego ludzi do pewnych działań, aby osiągnąć pewne korzyści polityczne lub społeczne. Ponadto, aby móc zakwalifikować atak jako cyberterroryzm, powinien on być dokonany w wyniku przemocy wobec osób lub mienia lub przynajmniej powodować znaczne szkody, aby wywołać strach. Przykładami takich ataków mogłyby być te, które prowadzą do śmierci lub obrażeń ciała, powodują eksplozje lub straty gospodarcze. D. Denning[251] twierdzi, że poważne ataki na infrastrukturę krytyczną mogą być również uznane za akty cyberterroryzmu, w zależności od ich wpływu. Z kolei ataki, które zakłócają nieistotne usługi lub są przede wszystkim kosztowne, do nich nie należą[252].

Należy stwierdzić, że pojęcie „cyberterroryzm" jest używane w kontekście politycznie umotywowanego ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów w szerokim rozumieniu tego słowa[253]. Przytoczone definicje dowodzą, że cyberterroryzm[254] pojmowany jest na świecie w dwojaki sposób. Według jednej koncepcji od terroryzmu klasycznego odróżnia go jedynie użycie technologii informatycznych w celu przeprowadzenia zamachu, druga koncepcja kładzie nacisk na systemy komputerowe jako cel ataków, a nie narzędzie do ich przeprowadzenia. Wydaje się, że prawdziwa definicja powstaje dopiero po połączeniu obu tych podejść[255].

Pojęcie cyberprzestępczości pojawia się coraz częściej w literaturze przedmiotu, choć należy zaznaczyć, że nie doczekało się ono jeszcze normatywnego ustalenia. Cyberprzestępczość określana jest jako podkategoria przestępczości komputerowej, obejmująca wszelkie rodzaje przestępstw, do których popełnienia użyto Internetu lub innych sieci komputerowych, przy czym komputery i sieci komputerowe mogą służyć do popełniania przestępstw na kilka sposobów: jako narzędzie przestępstwa, jako cel przestępstwa lub do realizacji innych zadań dodatkowych (np. przechowywania danych uzyskanych w wyniku przestępstwa)[256]. Mieszczą się tu zatem wszelkie ataki kierowane przeciwko połączonym systemom komputerowym i mające na celu uniemożliwienie im prawidłowego działania lub przeciwko danym przechowywanym w formie elektronicznej na pojedynczym komputerze bądź też kilku połączonych wspólną siecią. Najbardziej charakterystyczną cechą cyberprzestępczości jest to, że poszczególne czyny mogą być dokonywane za pomocą komputera podłączonego do Internetu lub sieci intranetowych[257].

TABELA 3.2. Podstawowe rodzaje cyberzagrożeń

Zjawisko	Charakterystyka
Cyberprzemoc	Wykorzystanie cyberprzestrzeni w celu wymuszenia odbioru niepożądanych komunikatów zawierających informacje (dane, obrazy, treści) sprzecznych z wartościami adresata.
Cyberprzestępstwo	Wykorzystanie cyberprzestrzeni w celu dokonania aktów kryminalnych pospolitych i zorganizowanych skierowanych na zasoby osób prywatnych i/lub organizacji (instytucji).

Cyberinwigilacja	Wykorzystanie cyberprzestrzeni w celu kontroli i/lub pozyskiwania informacji o zachowaniach i działaniach obywateli (społeczności, społeczeństwa) – efekt Wielkiego Brata.
Cyberterroryzm	Wykorzystanie cyberprzestrzeni w celu działań terrorystycznych (państwowych i pozapaństwowych).
Cyberautokratyzm	Wykorzystanie cyberprzestrzeni w życiu politycznym państwa niezgodnie z zasadami demokracji liberalnej (przeciwieństwem jest cyberdemokracja).
Cyberwojna	Wykorzystanie cyberprzestrzeni w celu realizacji działań politycznych realizowanych przez siły zbrojne (*cyberwarriors*) i skierowanych na zasoby oraz struktury państwa przeciwnika (również w działaniach innych niż wojna).

Źródło: M. Górka (red.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa XXI wieku*, Warszawa 2014, s.71.

Mianem cyberprzestępczości określa się takie formy posługiwania się sieciami telekomunikacyjnymi, siecią komputerową, Internetem, których celem jest naruszenie jakiegokolwiek dobra chronionego prawem[258]. Cyberprzestępczość odróżnia od klasycznej przestępczości przede wszystkim działanie w środowisku związanym z technologią komputerową i wykorzystanie sieci komputerowych do popełniania przestępstwa[259]. Jej wyróżnikiem nie jest natomiast ochrona wspólnego dobra[260]. Dzisiaj niemal każda nielegalna działalność ma odzwierciedlenie w Internecie. Jego globalny charakter umożliwił niezwykle szybką komunikację i przeniesienie większości form aktywności człowieka do sieci, także i tych negatywnie odbieranych. Coraz powszechniej mówi się o cyberprzestrzeni jako nowej przestrzeni społecznej, w której występują te same problemy co w świecie rzeczywistym. Cyberprzestępczość jest zatem nowoczesną odmianą przestępczości, wykorzystującą możliwości technik cyfrowych i środowiska sieci komputerowych.

Cyberprzestępczość jest zjawiskiem stosunkowo nowym, rozprzestrzeniającym się w zawrotnym tempie w społeczeństwach dobrze zinformatyzowanych i usieciowionych. Stanowi zagrożenie bardzo poważne i trudne do zwalczania. Decydują o tym szczególne właściwości, jakimi cechuje się to zjawisko[261]. Pierwsza z cech powoduje, że działania cyberprzestępców z łatwością przenikają bariery, jakimi są granice państw. Bardzo często cyberprzestępcy prowadzą swoje działania w jednym miejscu, ich skutki zaś ujawniają się zupełnie gdzie indziej, w miejscu oddalonym o setki kilometrów, nierzadko w innym kraju, na innym kontynencie. Uniemożliwia to określenie systemu prawnego, według którego miałoby następować ściganie takich przestępstw, a jednocześnie znacznie utrudnia wyznaczenie podmiotów odpowiedzialnych za podejmowanie działań ochronnych i zapobiegawczych. Kolejna cecha to anonimowość, która nie ułatwia szybkiego ustalenia sprawców przestępstw oraz wykrycia sposobów ich działania[262]. Nie jest to jednak niemożliwe, ale wymaga podjęcia żmudnych poszukiwań i wdrożenia dobrze przemyślanych i zaplanowanych działań. Wygoda i szybkość, które zapewnia korzystanie z nowoczesnych technik komputerowych i sieciowych, sprzyjają błyskawicznemu upowszechnianiu tej formy przestępczości w państwach najbardziej rozwiniętych[263].

Wszystko to sprawia, że ochrona przed zagrożeniami związanymi z cyberprzestępczością jest niezwykle trudna i wiąże się z podejmowaniem licznych przedsięwzięć, w tym także wymagających wieloaspektowej i szeroko zakrojonej współpracy międzynarodowej. Dla skuteczności tej ochrony niezbędna jest współpraca poszczególnych państw w celu ustalenia wspólnej polityki przeciwdziałania cyberprzestępczości, a następnie jej konkretyzacja przez określenie niezbędnych priorytetów oraz jednolitych zasad wspólnego działania. Tak wyznaczone zasady ogólne muszą zostać wprowadzone do prawa wewnętrznego państw, stając się podstawą instytucjonalnego i funkcjonalnego systemu instrumentów do walki z

cyberprzestępczością. Stworzenie skutecznego systemu przeciwdziałania cyberprzestępczości nie jest proste, wymaga pogłębionej analizy zjawiska w dłuższej perspektywie, a przy tworzeniu takiego systemu mogą wystąpić liczne problemy z dostosowaniem ogólnych wytycznych prawa międzynarodowego bądź unijnego do prawa wewnętrznego poszczególnych państw.

Cyberprzestrzeń wchodzi w relacje z cyberobiektami, gdyż dzięki odpowiedniemu oprogramowaniu i połączeniom kablowym umożliwia przesyłanie informacji z jednego miejsca w drugie, powodując pojawienie się cyberobiektów na ekranach komputerów. Żądając dostępu do określonego cyberobiektu, np. strony www, taki obiekt odszukiwany jest w miejscu swego składowania, a następnie przesyłany przez cyberprzestrzeń i reinterpretowany przez przeglądarkę odbiorcy w celu wyświetlenia go na ekranie zgodnie z intencjami autora. W cyberprzestrzeni zatem odbywają się dekonstrukcja i rekonstrukcja cyberobiektów, co wskazuje na to, że cyberprzestrzeń ma cechy przestrzeni zarówno absolutnej, jak i relatywnej[264].

Polityka cyberbezpieczeństwa definiuje sposoby korzystania z kont użytkowników i danych przechowywanych w systemie, zapewniając właściwą ochronę informacji instytucji[265]. W każdej organizacji występują informacje chronione, np. dane osobowe, informacje finansowe oraz informacje jawne, np. informacje marketingowe[266]. Polityka ochrony cyberprzestrzeni państwa kierowana jest do wszystkich użytkowników cyberprzestrzeni w obrębie danego państwa i poza jego terytorium, w miejscach, gdzie funkcjonują jego przedstawiciele. Jej zadaniem jest zobowiązanie organów administracji rządowej do stworzenia systemu ochrony cyberprzestrzeni państwa, który będzie szybko reagował i zapobiegał powstaniu cyberataku, a w przypadku dojścia do tego zdarzenia potrafił sprawnie pokonać przeprowadzony atak cybernetyczny.

W literaturze przedmiotu obok pojęcia cyberprzestępstwa można spotkać inne, np. „przestępstwo komputerowe", „przestępstwo związane z wykorzystaniem komputera", „przestępstwa internetowe". Pojęcia te, często używane zamiennie, nie zostały dokładnie zdefiniowane z uwagi na brak powszechnej zgody co do ich zakresu znaczeniowego. Jak podkreśla A. Adamski[267], o przestępstwach komputerowych mówi się w aspekcie zarówno materialnoprawnym, jak i procesowym. W świetle przepisów prawa karnego materialnego można wyróżnić dwa rodzaje przestępstw komputerowych. W pierwszej grupie znajdują się wszystkie zamachy skierowane na systemy, przetwarzane i utrzymywane w nich dane oraz programy komputerowe. Systemy i sieci komputerowe są w tym przypadku przedmiotem lub środowiskiem ataku. Do drugiej grupy zaliczamy natomiast przestępstwa dokonane z wykorzystaniem komputera w celu naruszenia dóbr tradycyjnie chronionych przez prawo karne.

Państwa – cyberagresorzy prowadzą zorganizowane działania walki informacyjnej i cyberszpiegostwa. Ocena analizy cyberzagrożeń prowadzonych przez znawców przedmiotu wskazuje, że głównymi państwami przeprowadzającymi ataki w cyberprzestrzeni są: Chiny, Rosja, Stany Zjednoczone, Iran i Korea Północna. Zdaniem specjalistów Chiny systematycznie rozwijają sieciowe techniki walki i tym samym zmniejszają w tej dziedzinie dominację Stanów Zjednoczonych. Chińska armia tworzy oddziały hakerskie, werbując najzdolniejszych informatyków. Z ujawnionych przez WikiLeaks depesz amerykańskich dyplomatów w Pekinie wynika, że ataki chińskich hakerów motywowane są politycznie. W przekazach można było przeczytać, że „ambasadzie udało się ustalić, że akcja jest koordynowana przez chińskie Narodowe Biuro Informacji, główny organ wykonawczy chińskich władz w zakresie m.in. mediów i Internetu"[268]. Jednocześnie Chiny informują, że same są celem licznych

cyberataków, w których wyniku w ostatnich latach ponad milion chińskich kont znalazło się pod kontrolą podmiotów zagranicznych.

Ważnym momentem przełomowym w cyberatakach były lata 2016–2017, kiedy wykorzystano ramsomware[269]. Był to początek kolejnej odsłony cyberprzestępstw. Jednym z takich przykładów jest Mirai. 21 października 2016 r. dokonano ataku DDoS na system zarządzania DNS, na skutek czego oparte na nim serwisy stały się niedostępne w Stanach Zjednoczonych. Dotknęło to PayPala, Twittera, Netflixa, serwisu Spotify czy usług internetowych PlayStation. Urządzenia, których nigdy nie zabezpieczono i dla których nie istniały programy antywirusowe, nagle zostały zainfekowane na dużą skalę. Następnie wyszukiwały one podobne pliki w celu przekazania infekcji. Ta armia urządzeń zombie, opierająca się na szkodliwym programie Mirai (j. jap. – przyszłość) nieustannie się rozrastała, czekając cały czas na instrukcje. Ostatecznie dostawca, firma Dyn, odzyskał swoją sprawność, ale skala ataku Mirai skłoniła świat do zastanowienia się nad kwestiami bezpieczeństwa inteligentnych urządzeń[270].

Kolejnym przykładem jest WannaCry, który można nazwać „prawdziwą epidemią" ponieważ do ataków hakerskich doszło aż w 150 państwach[271]. Ich celem były szpitale, firmy telekomunikacyjne, banki. Hakerzy użyli narzędzia skradzionego z agencji wywiadowczej USA, domagając się opłaty za odblokowanie komputerów. Szpitale w Wielkiej Brytanii nawet zostały zmuszone odsyłać pacjentów. Europol określił cyberatak na organizacje na całym świecie mianem „bezprecedensowego", zapowiadając jednocześnie międzynarodowe dochodzenie w celu wykrycia sprawcy[272]. Hakerzy wykorzystali lukę wykrytą w systemie Microsoftu i opracowaną przez NSA, amerykańską agencję wywiadowczą koordynującą m.in. zadania wywiadu elektronicznego. O luce w systemie Microsoft wiedziało tylko NSA, jednak agencja nie poinformowała o niej korporacji. Metody jej wykorzystania zostały wykradzione z NSA przez grupę nazywającą się Shadow Brokers i opublikowane w Internecie.

Główny obszar zainteresowań zaangażowania Rosji w cyberprzestrzeni stanowi obecnie prowadzenie wybranych działań w ramach walki informacyjnej, czego doświadczyły: Estonia (2007)[273], Gruzja (2008)[274] oraz Stany Zjednoczone[275]. O znaczeniu cyberzagrożeń dla bezpieczeństwa Rosji może świadczyć fakt, że w doktrynie bezpieczeństwa informacyjnego Federacja Rosyjska zastrzega sobie prawo do odwetowego uderzenia jądrowego na siły i środki walki informacyjnej potencjalnego przeciwnika[276]. Według Rosjan „wojna informacyjna to walka między państwami w przestrzeni informacyjnej w celu uszkodzenia systemów informacyjnych, przetwarzania danych oraz zasobów, struktur newralgicznych i innych, zachwianie systemów politycznych, ekonomicznych i społecznych, jak również narzucenia danemu państwu podejmowania zadań w interesach strony przeciwnej"[277]. Część państw (zwłaszcza cybermocarstaw takich jak Rosja, Chiny czy USA) dostrzegła ogromny potencjał cyberprzestrzeni. Coraz częściej przestrzeń ta zaczęła być wykorzystywana do realizacji polityki państwa, propagandy, inwigilacji, ale również działań militarnych. Wydaje się, że w przyszłości państwa, kierując się potencjalnymi korzyściami (uzyskanie newralgicznych informacji, tajnych danych, dezinformacja i paraliż przeciwnika) coraz częściej (bardziej lub mniej jawnie), będą wykorzystywać cyberprzestrzeń do realizacji swojej polityki. Głównym celem ataków w cyberprzestrzeni, w tym o cechach cyberterrorystycznych, są przede wszystkim Stany Zjednoczone. Zdecydowana większość odbywa się ze strony Chin. Ich celem są instytucje zarówno rządowe, wojskowe, jak i mieszkańcy.

3.2
UWARUNKOWANIA ZAGROŻEŃ CYBERTERRORYSTYCZNYCH W UNII EUROPEJSKIEJ

3.2.1. UWARUNKOWANIA ZEWNĘTRZNE

Ukształtowany na początku lat 90. XX w. ład międzynarodowy przyjął układ policentryczny. Jego podstawą stały się Stany Zjednoczone Ameryki oraz mocarstwa regionalne, za które uznawano Rosję, Chiny, Japonię, Unię Europejską oraz tzw. krąg islamski. W ramach tego globalnego układu sił funkcjonowały trzy grupy państw:

- państwa postindustrialne – pierwsza fala (Ameryka Północna, Europa Zachodnia, tzw. Pierścień Pacyfiku),
- państwa „późno lub nowo industrializowane" – druga fala,
- państwa współczesnego kręgu przedindustrialnego – trzecia fala.

Zakończenie rywalizacji dwóch bloków militarnych, jakie nastąpiło na początku lat 90. ubiegłego wieku, miało – w przekonaniu polityków i politologów – zapoczątkować erę stabilności w kontaktach międzynarodowych określaną jako „koniec historii"[278]. Jego immanentną cechą był zanik czynników konfliktogennych, prowadzących do wybuchu wojen o charakterze kontynentalnym lub globalnym. Jednak nawet twórca tej tezy amerykański politolog Francis Fukuyama[279] po kilku latach uznał ją za błędną. Likwidacja „systemu zimnowojennego", która sprowadzała się do rozpadu dwóch i poważnego osłabienia trzeciej „warstwy imperium moskiewskiego", doprowadziła bowiem do znacznych przeobrażeń ładu międzynarodowego. Charakteryzowały go następujące procesy:

- zanik bipolarnego globalnego układu sił,
- przeobrażenia funkcji mocarstwowości,
- generalna zmiana cywilizacyjna, w której zasadniczą rolę odgrywa globalizacja wraz z rewolucją informatyczną oraz wzrostem znaczenia organizacji międzynarodowych i pozapaństwowych[280].

Przeobrażenia systemu zimnowojennego ograniczyły do minimum zagrożenie wybuchu konfliktu zbrojnego między państwami pierwszej lub pierwszej i drugiej grupy państw. W ten sposób, niejako samoczynnie, zmniejszyło się znaczenie globalnego układu świata Wschód – Zachód, którego główną linią podziału była kwestia ideologii. Zdecydowanie większe znaczenie zaczęły odgrywać czynniki społeczno-ekonomiczne, a zwłaszcza rozwarstwienie na linii Północ – Południe. Asymetria poziomu rozwoju poszczególnych regionów globu przybrała jednak cechy konfliktogenne, a czynnikami kryzysogennymi stały się – obok potencjału militarnego i gospodarczego – także kwestie religijne, demograficzne, społeczne (bezpieczeństwo socjalne) oraz ideologiczne. Pierwszą, naturalną konsekwencją zaprezentowanych przeobrażeń ładu międzynarodowego było rozprzestrzenienie się skrywanych lub ograniczanych przez mocarstwa sporów o charakterze narodowościowym. Ich źródeł należy poszukiwać w czynnikach kulturowych, demograficznych i społecznych oraz w restytucji poczucia przynależności narodowościowej[281].

Po zakończeniu zimnej wojny i rozpadzie układu dwubiegunowego znacznie spadły skala, zakres i natężenie tradycyjnych zagrożeń militarnych (odnosiło się to przede wszystkim do obszaru transatlantyckiego). Zmniejszenie ryzyka wybuchu wojny ogólnoświatowej natomiast nie przełożyło się na złagodzenie konfliktów regionalnych czy lokalnych – te nawet się

zaostrzyły. Jednocześnie zagrożenia asymetryczne rozwinęły się lub uzyskały nowe formy. Przyczyną tego było wiele czynników, które nawzajem się wzmacniały, np. przemiany ładu międzynarodowego, nowe podziały, konflikty i in.

Koniec dotychczasowego ładu oznaczał, że mniej liczące się czynniki zyskały na znaczeniu jako uwarunkowania kształtu międzynarodowego środowiska bezpieczeństwa, np. terroryzm, a tym samym jako determinanty rozwoju organizacji terrorystycznych. W wyniku rozpadu układu bipolarnego USA zyskały więc pozycję supermocarstwa globalnego[282].

Wraz z zakończeniem zimnej wojny wyznacznikiem kształtu stosunków międzynarodowych zaczęło być zróżnicowanie kulturowo-cywilizacyjne[283]. Odnosi się ono przede wszystkim do odmienności zarówno między państwami, jak i społeczeństwami należącymi do różnych kręgów kulturowych czy cywilizacyjnych[284].

Należy podkreślić, że bezpieczeństwo globalne i lokalne uwarunkowane jest wieloma czynnikami, w tym politycznymi. Polityki wewnętrzna i zewnętrzna prowadzone przez dany podmiot wpływają na poczucie bezpieczeństwa obywateli oraz warunkują jego miejsce w rzeczywistości międzynarodowej. Bezpośrednie zagrożenie jest związane z możliwością wystąpienia wojny, ze stanem pozostawania w stanie wojny lub z oficjalnym prowadzeniem konfliktu militarnego. Kryzys polityczny, gospodarczy, społeczny czy kulturowy może również wpływać na sytuację międzynarodową państwa, a na potencjalne zagrożenia i wyzwania dotyczące kształtowania bezpieczeństwa państwa mają również wpływ jego relacje z sąsiadami[285].

Jak słusznie zauważa Carlo Jean[286], szeroko rozumiany „Zachód", mając świadomość, że na jego obszarze konsumuje się 70% produkcji światowej, czuł się zobowiązany do przeciwdziałania zacofaniu gospodarczemu, walki z głodem i epidemiami oraz przejawom walk etnicznych. Jednak sama reakcja na konflikt oraz jej forma stały się w tym okresie nie tyle obowiązkiem, ile funkcją własnej (narodowej) polityki. Doprowadziło to do wykreowania w 1996 r. pojęcia „wojny słusznej". Po raz pierwszy pojęcie to zdefiniowano w doktrynie bezpieczeństwa Stanów Zjednoczonych, uznając, że zakres zaangażowania własnych sił zbrojnych w misjach zaprowadzania pokoju jest w znacznym stopniu uzależniony od kształtu interesów narodowych USA. Tę decyzję administracji Billa Clintona należy uznać za początek ery „świata jednowymiarowego", która doprowadziła pośrednio do znaczących przeobrażeń w globalnym systemie bezpieczeństwa[287].

Przekonanie establishmentu politycznego Stanów Zjednoczonych o konieczności utrzymania prawa do swobody podejmowania decyzji w imię interesu narodowego oraz globalnego promowania tzw. amerykańskich wartości doprowadziło bowiem do całkowitego załamania globalnego systemu pomocy humanitarnej realizowanego pod auspicjami Organizacji Narodów Zjednoczonych. Zastąpiono go międzynarodową aktywnością o charakterze polityczno-militarnym, definiowaną jako „dyplomacja prewencyjna". Wykorzystując instrumentarium „dyplomacji prewencyjnej", nie zlikwidowano żadnego ze źródeł i przyczyn konfliktów. Wręcz przeciwnie, wywieranie przez cywilizację zachodnią silnego wpływu i bezwzględne upowszechnianie własnych wzorców cywilizacyjnych doprowadziły do powstania fali fundamentalizmu, wzrostu poczucia odrębności etniczno-kulturowej oraz agresywnych odmian nacjonalizmu. Można wręcz stwierdzić, że negatywną konsekwencją podejmowanych misji stabilizacyjnych jest pojawienie się nowych zagrożeń bezpieczeństwa. Wśród nich należy wymienić[288]:

- przejęcie władzy w państwach przez „warlordów" – przywódców partyzanckich, grup przestępczych czy gangów, którzy uzyskali kontrolę nad obszarem państwa lub częścią jego terytorium,
- „upaństwowienie" procederu handlu bronią, niewolnikami,

- wystąpienie masowych migracji jako konsekwencji konfliktów lokalnych,
- „przeniesienie" skutków i następstw konfliktów na ludność cywilną.

Zagrożenia związane z cyberprzestrzenią stały się jednym z głównych tematów polityki wielu państw, organizacji międzynarodowych, w tym również Unii Europejskiej, ponieważ cyberprzestrzeń staje się coraz ważniejszym wymiarem systemu międzynarodowego, a UE dostosowuje swoją strategię w tym obszarze.

Brunon Hołyst[289] w swoich rozważaniach na temat terroryzmu podkreśla, że cyberprzestrzeń jest wykorzystywana również do mobilizacji czasowej cyberterrorystów, czyli osób popierających, lecz nie związanych bezpośrednio i stale z grupami terrorystycznymi. Wzywa się ich wówczas do określonego zachowania się. Nie mniej istotna jest możliwość oddziaływania na systemy komputerowe i teleinformatyczne przeciwnika przez używanie e-bomb, wirusów, robaków internetowych i włamań hakerów.

Ataków cyberterrorystycznych nie należy kojarzyć wyłącznie z grupami terrorystycznymi. Mogą się ich dopuścić również inne podmioty, w tym państwa, wówczas atak cybernetyczny może być działaniem szpiegowskim lub elementem działań wojennych prowadzącym do dezinformacji przeciwnika. Przed inwazją lądową państwa mogą dopuścić się ataków cyberterrorystycznych na urządzenia infrastruktury krytycznej, serwery państwowe lub wojskowe przeciwnika. Mimo że sprawcy cyberataków niejednokrotnie pozostają anonimowi, często uważa się, że stoją za nimi Chiny, Korea Północna, Rosja, Indie czy Izrael. Przykładem takich działań może być skierowanie w 2008 r. ataku DDoS na serwery publiczne Gruzji: stron www prezydenta, Ministerstwa Spraw Zagranicznych, Narodowego Banku Republiki Gruzji, banków komercyjnych i mediów. Sprawcami cyberataków mogą być również zorganizowane grupy (ruchy narodowowyzwoleńcze, podmioty gospodarcze operujące w sieciach teleinformatycznych) bądź też pojedynczy sprawcy (hakerzy, aktywiści, krakerzy, frustraci, szpiedzy, wandale), którzy chcą sprawdzić swoje umiejętności, włamując się do wysoce strzeżonych systemów[290].

Ernest Lichocki[291] dzieli cyberterroryzm na państwowy i niepaństwowy. Do pierwszego zalicza walkę informacyjną, walkę z terroryzmem i organizacjami terrorystycznymi, walkę z zorganizowaną przestępczością, w tym z handlarzami narkotyków oraz działalność resortów siłowych państwa (służb ochrony państwa). Do cyberterroryzmu niepaństwowego należą wandale, hakerzy, krakerzy, aktywiści, haktywiści, szpiedzy, frustraci, działalność organizacji terrorystycznych oraz działalność ruchów narodowowyzwoleńczych.

Należy przypomnieć, że w przypadku państw europejskich terroryzm miał przede wszystkim charakter wewnętrzny, a cyberterroryzm jest co do zasady zjawiskiem zewnętrznym. To spowodowało następstwa dwojakiego rodzaju – państwa uznawały i w dużej mierze nadal uznają przeciwdziałanie terroryzmowi za zagadnienie należące do ich wyłącznej kompetencji. Współpracę międzynarodową w tym zakresie postrzegają jako konieczną, ale stanowiącą jedynie uzupełnienie i poszerzanie zdolności do walki z terroryzmem[292]. Dopiero po wejściu w życie Traktatu z Maastricht polityka antyterrorystyczna znalazła się oficjalnie w trzecim filarze Unii Europejskiej, czyli współpracy międzyrządowej w dziedzinie sprawiedliwości i spraw wewnętrznych. Umiejscowienie tej gałęzi polityki właśnie w tym filarze spowodowało, że od początku współpraca była często mało efektywna. Wprawdzie w programie ramowej współpracy w sprawach należących do wymiaru sprawiedliwości i spraw wewnętrznych polityka antyterrorystyczna stała się przedmiotem wspólnego zainteresowania wszystkich państw członkowskich, ale w pierwszych latach obowiązywania tego traktatu Unia Europejska prowadziła politykę nastawioną na konsolidację wewnętrzną przy pewnym zaniedbaniu stosunków z państwami trzecimi[293]. Właśnie w obszarze III filaru okazało się, że

bez kooperacji z państwami ościennymi UE nie uda się osiągnąć założonych celów. O tym fakcie przesądziły także niewielka rola Komisji Europejskiej i marginalizacja Parlamentu Europejskiego. Istniało przekonanie, że współpraca na poziomie międzyrządowym jest wystarczająca. Od momentu wejścia w życie Traktatu z Amsterdamu i utworzenia strefy wolności, bezpieczeństwa i sprawiedliwości państwa członkowskie wzmocniły środki działań przez integrację instrumentów odnoszących się do kontroli na granicach zewnętrznych, azylu i migracji w ramach Wspólnoty oraz zapobieganie i zwalczanie przestępczości międzynarodowej.

Rosnące zagrożenia cybernetyczne i postrzeganie niepewności cybernetycznej powodowały wzrost nieufności wśród obywateli, potencjalnie powstrzymując europejską gospodarkę w miarę jej cyfryzacji. Komisja Europejska, uznając, że bezpieczeństwo cybernetyczne stanowi kluczowy element strategii rynku, wskazała na potrzebę ochrony sieci energetycznych, infrastruktury krytycznej UE i skutecznego reagowania na zagrożenia cybernetyczne oraz na potrzebę korzystania z istniejących krajowych i unijnych strategii regulacji w zakresie bezpieczeństwa cybernetycznego[294]. Podstawą reformy miały być działania przewidziane w strategii cyberbezpieczeństwa oraz główny filar strategii – dyrektywa o bezpieczeństwie sieci i informacji (dyrektywa NIS). Szybki rozwój usług komunikacyjnych związany z przesyłaniem olbrzymiej ilości danych stawia wiele wyzwań przed podmiotami odpowiedzialnymi za ich przesyłanie, przechowywanie i przetwarzanie. Dodatkowo automatyzacja sieci energetycznych i budowa tzw. sieci inteligentnych powoduje również zwiększenie ilości gromadzonych danych. Ta szeroko rozumiana informatyzacja działalności związanej z dostarczaniem energii elektrycznej sprawia, że jest ona narażona na cyberataki. Konieczne jest zatem rozwijanie narzędzi, które pozwolą w maksymalnie zabezpieczyć prowadzenie działalności dystrybucyjnej oraz odbiorców energii.

Według niektórych uczonych do połowy tego wieku sztuczna inteligencja będzie poza ludzkim zrozumieniem i kontrolą[295]. Jeśli tak się stanie, ludzkość napotka bezprecedensowe problemy prawne, a antropocentryczny punkt widzenia dzisiejszych systemów prawnych nie pozwala ludzkości rozwiązać tych problemów[296].

Chociaż w 2005 r. Rada UE przyjęła strategię w dziedzinie walki z terroryzmem (w tym także z cyberterroryzmem), aby globalnie zwalczać terroryzm i zapewnić Europie bezpieczeństwo przy jednoczesnym poszanowaniu praw człowieka i umożliwieniu obywatelom UE życia w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, to strategia walki ze zjawiskiem cyberterroryzmu została przyjęta w UE w 2013 r. Ważny był również *Program sztokholmski*, który wyznał w dziedzinie sprawiedliwości i spraw wewnętrznych cele strategiczne na lata 2010–2014[297].

Następnie UE przyjęła *Strategię globalną UE* w 2016 r., co wyraźnie ożywiło działania dotyczące polityki bezpieczeństwa związane z polityką antyterrorystyczną (w tym cyberterrorystyczną). Obecna *Strategia UE* z 2016 r. identyfikuje pięć priorytetów[298]. Kolejnym ważnym krokiem w jej wdrażaniu jest z pewnością ustanowienie i uruchomienie pod koniec 2017 r. projektu Stałej Współpracy Strukturalnej, czyli PESCO[299]. *Strategia globalna UE* wdrażana jest na trzech polach: politycznym, ekonomicznym i międzynarodowym. Pole polityczne to implementacja w dziedzinie bezpieczeństwa i obrony koordynowana przez Wysoką Przedstawiciel ds. WPBiO. Pole ekonomiczne stanowi europejski plan działań na rzecz obronności realizowany przez Komisję Europejską. Trzecie pole międzynarodowe to realizacja przez wszystkie podmioty UE porozumienia o współpracy z NATO. Najważniejszym dokumentem wdrożeniowym wobec strategii jest *Plan implementacji w dziedzinie bezpieczeństwa i obronności*[300]. W jego ramach ustanowiono nowy poziom UE dotyczący bezpieczeństwa i obronności w odniesieniu do trzech podstawowych zadań: reagowania na

zewnętrzne konflikty i kryzysy, budowania zdolności partnerów, ochrony UE i jej obywateli. Przy każdym z tych założeń strategia podkreśla wagę współpracy z państwami trzecimi i instytucjami międzynarodowymi.

We wrześniu 2017 r. KE rozpoczęła prace nad strategią bezpieczeństwa cybernetycznego z 2013 r., wydając dokument roboczy przedstawiający jej ocenę[301]. W nowym dokumencie po raz pierwszy zawarto potrzebę „utrzymania i rozwoju przez UE podstawowych zdolności do zapewnienia bezpieczeństwa gospodarki cyfrowej, społeczeństwa i demokracji". Celem polityki stało się zmniejszenie fragmentaryzacji rynku, a także rozwinięcie zdolności gospodarczych i poprawa działań wobec incydentów cybernetycznych. Konkretne kroki polityczne podjęto w 2017 r. Należy tu wymienić działania unijne dotyczące partnerstwa publiczno-prywatnego na rzecz badań i innowacji. Stwierdzono potrzebę wprowadzenia nowego europejskiego systemu certyfikacji, który zagwarantuje, że produkty i usługi w świecie cyfrowym będą bezpieczne w użyciu.

KE i Wysoki Przedstawiciel, chcąc stworzyć właściwe narzędzia do walki z atakami cybernetycznymi, zaproponowali instrumenty dające wzmocnienie bezpieczeństwa w polityce ochrony cybernetyczni. Wprowadzono zaktualizowaną strategię bezpieczeństwa cybernetycznego, której celem jest usprawnienie wspólnego podejścia państw członkowskich do zjawiska cyberzagrożeń. W odnowionej strategii zalecono również utworzenie europejskiego centrum badań naukowych i kompetencji w dziedzinie cyberbezpieczeństwa oraz wskazano na potrzebę posiadania umiejętności przez organy unijne w celu przeprowadzenia skoordynowanych reakcji na dużą skalę wobec incydentów i kryzysów związanych z bezpieczeństwem cybernetycznym.

Sytuacja ta zmieniła się za sprawą wprowadzenia dyrektywy NIS. Akt ten formalnie stworzył sieć zespołów reagowania państw członkowskich na incydenty komputerowe (CSIRT), a sekretariat tej sieci zapewnia ENISA. Głównym celem agencji jest wspieranie państw członkowskich we wdrażaniu dyrektywy NIS. Agencja otrzymała nowe zadania i zasoby w takich dziedzinach, jak współpraca operacyjna i certyfikacja bezpieczeństwa technologii informacyjno-komunikacyjnych (ICT) w celu podejmowania działań, które będą odzwierciedlać nowe potrzeby w zakresie bezpieczeństwa cybernetycznego. ENISA odegra zatem ważną rolę w dziedzinie unijnej polityki certyfikacji bezpieczeństwa cybernetycznego dzięki przygotowaniu we współpracy z organami certyfikującymi państw członkowskich systemów certyfikacji bezpieczeństwa cybernetycznego[302].

Jednym z zadań polityki UE w zakresie cyberbezpieczeństwa jest wzmocnienie zdolności i współpracy w obszarze bezpieczeństwa cybernetycznego w celu zapewnienia takiego samego poziomu rozwoju we wszystkich państwach członkowskich na ataki cybernetyczne pochodzące zarówno z zewnątrz, jak i wewnątrz. Aby zrealizować to wyzwanie, Parlament Europejski i Rada UE wprowadziły w 2016 r. dwa nowe akty prawne, które obecnie kształtują podstawowe ramy europejskiego bezpieczeństwa cybernetycznego w wymiarze społeczno-gospodarczym.

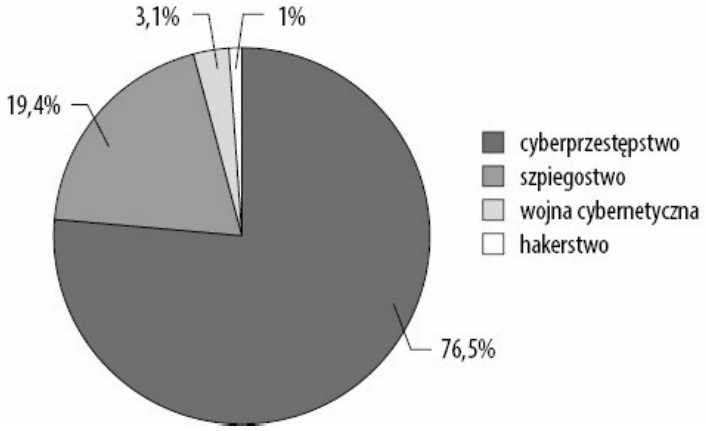
Pierwszym z nich jest dyrektywa w sprawie bezpieczeństwa sieci i informacji (NIS), która ma na celu zapewnienie sprawnego funkcjonowania europejskiego rynku wewnętrznego[303]. Wymaga ona także, aby wszystkie państwa UE posiadały zdolności w zakresie cyberbezpieczeństwa i współpracowały ze sobą na poziomie strategicznym i operacyjnym.

Celem dyrektywy NIS jest stworzenie równych szans wśród państw członkowskich UE, ustanawiając wymóg posiadania właściwego organu ds. cyberbezpieczeństwa, jak również zdolność do reagowania na incydenty techniczne na poziomie krajowym. W dokumencie zachęca się do współpracy między państwami członkowskimi w celu ułatwienia wymiany informacji i współpracy operacyjnej w razie incydentów. Dyrektywa zatem koncentruje się na

zwiększeniu szybkości, regularności i centralizacji wymiany informacji między sektorami publicznym a prywatnym[304]. Dokument nie tworzy jednak centralnego europejskiego wykazu infrastruktury krytycznej ani nie wymaga wspólnych norm. Rządy poszczególnych państw są zobowiązane do współpracy i dzielenia się niektórymi informacjami, ale akt ten nie wprowadza wymogów obowiązkowej ogólnoeuropejskiej współpracy i mechanizmów wymiany informacji, które pierwotnie przewidywano.

Drugim ważnym aktem prawnym jest – wspomniane wcześniej – rozporządzenie w sprawie ochrony danych osobowych (RODO, inaczej GDPR)[305]. Nowe przepisy tworzy spójny, jednolity zbiór regulacji dla wszystkich przedsiębiorstw działających w UE, które przetwarzają dane osobowe obywateli UE. Celem tego rozporządzenia jest ochrona praw jednostki w związku z przetwarzaniem danych osobowych. Określa ono prawo dostępu do informacji, reguluje gromadzenie informacji, przetwarzanie i przekazywanie danych między podmiotami publicznymi oraz daje obywatelom prawo do „bycia zapomnianym", co wymaga od przedsiębiorstw usunięcia pewnych danych osobowych na wniosek obywatela.

Często porównuje się rozporządzenie GDPR i dyrektywę NIS. Należy jednak zwrócić uwagę na różnice z punktu widzenia polityki cyberbezpieczeństwa. Dyrektywa w sprawie bezpieczeństwa sieci i informacji kładzie większy nacisk na sprawne funkcjonowanie gospodarki. Jej jednym z podstawowych zadań jest pomoc przedsiębiorstwom skuteczniej zapobiegać atakom na infrastrukturę cyfrową, której sieć obejmuje wiele państw UE.

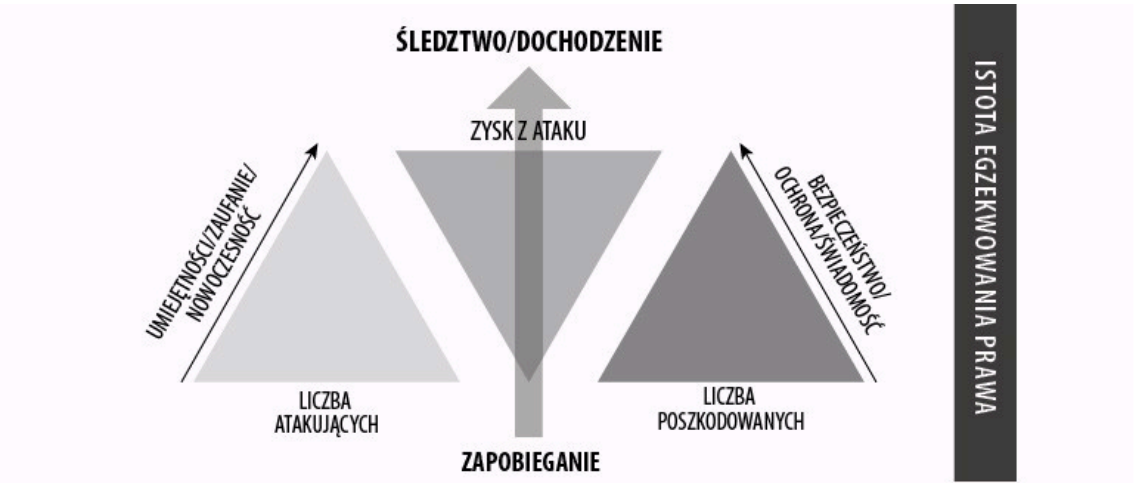


RYSUNEK 3.1
Uwarunkowania ataków w cyberprzestrzeni
Źródło: hackmageddon.com (dostęp: 7.06.2020).

Z danych przedstawionych na *rys. 3.1* wynika, że cyberprzestępstwo i cyberszpiegostwo są głównymi czynnikami motywacyjnymi do działania, stanowiąc 95,9%, cyberwojna i hakerstwo natomiast to zaledwie niewiele ponad 4%. Wynika to przede wszystkim z niematerialności cyberprzestrzeni i jej globalnego charakteru[306]. Co za tym idzie, nie obowiązują tu ograniczenia o charakterze fizycznym. Stosunkowo łatwo ukryć w niej również prawdziwą tożsamość sprawców incydentów teleinformatycznych. Brak tu nie tylko wywiadu strategicznego, ale także w wielu przypadkach możliwości zidentyfikowania osoby odpowiedzialnej za dany atak komputerowy. Jest to wbrew pozorom problem o fundamentalnym znaczeniu. Wskazanie podmiotu odpowiedzialnego za włamanie jest bowiem kwestią zasadniczą w przypadku przygotowania odpowiedniej reakcji politycznej, prawnej czy wojskowej.

Kolejną istotną cechą cyberprzestrzeni są relatywnie niskie koszty działania w niej i wyjątkowo wysoki zysk, co przedstawiono na *rys. 3.2*.

Z danych przedstawionych na *rys. 3.2* wynika, że przewagą cyberprzestępców są ich umiejętności, znajomość technologii i innowacyjnych rozwiązań cyberprzestrzeni. Z kolei słabością ofiar przestępstw terrorystycznych jest ich niewiedza i chęć posiadania ochrony (zabezpieczeń) internetowych. Cyberprzestępcy będą działać tak długo, aż poczynione nakłady (koszty) będą niższe od uzyskanych przychodów i dopóki luki w prawie oraz egzekucja prawa będą hakerom na to pozwalać. Trychotomia zjawiska cyberprzestępstwa polega na połączeniu tych trzech czynników – ścigania, zapobiegania i egzekucji prawa w celu zminimalizowania zjawiska cyberprzestępczości.

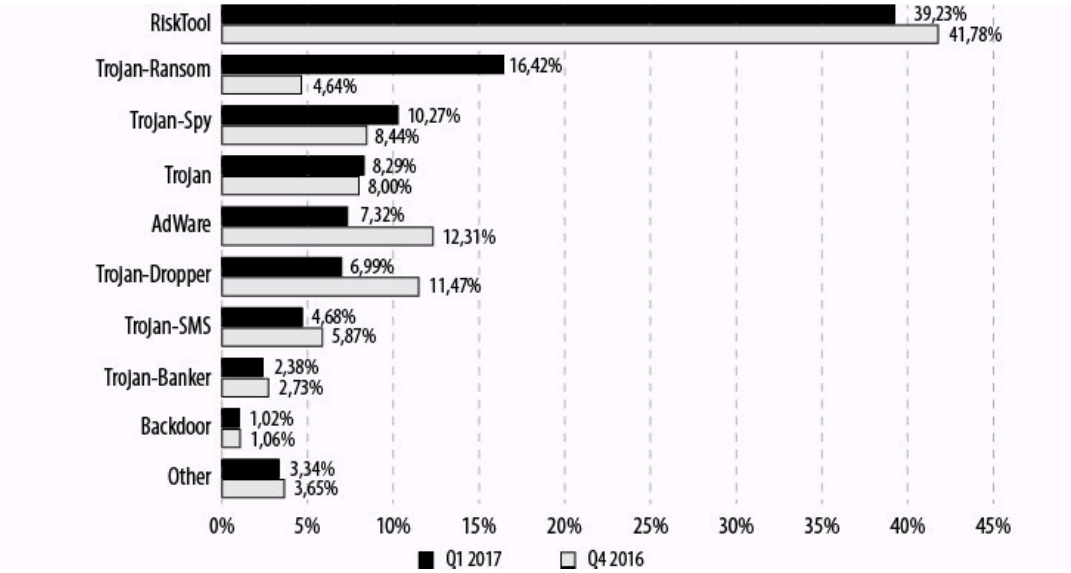


RYSUNEK 3.2
Trychotomia zjawiska cyberprzestępstwa

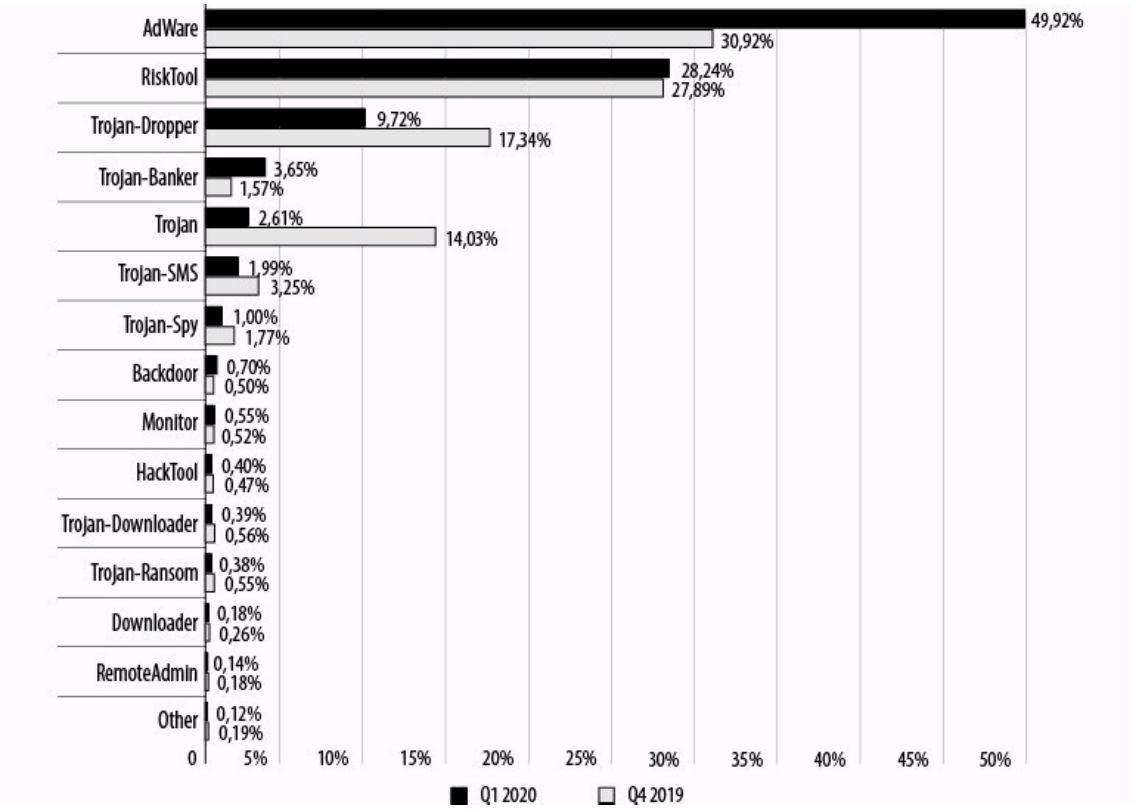
Źródło: Raport Europol SOCTA 2017 r., *European Union serious and organised crime. Threat assessment* (dostęp: 27.05.2020).

Należy również zauważyć, że nastąpiła zmiana adresata – ofiary cyberprzestępcy. Po okresie spokoju charakteryzującego koniec 2017 r. nastąpił powrót długotrwałych ataków: najdłuższy trwał 297 godzin (12,4 dni). Chociaż brakuje mu jeszcze do rekordu światowego, był to niewątpliwie długi atak, dłuższy miał miejsce w 2015 r.[307] Ofiary cyberprzestępców nie są już przypadkowe, często stają się nimi przedsiębiorcy i instytucje, np. banki.

Udział wszystkich innych długotrwałych ataków (co najmniej 50 godzin) zwiększył się ponad sześciokrotnie, z 0,10% do 0,63%. Wzrosła również liczba najkrótszych ataków (do 9 godzin): o ile wcześniej stanowiły one 85,5% wszystkich ataków, obecnie wynoszą 91,47%. Z kolei liczba ataków trwających od 10 godzin do trzech dni zmniejszyła się niemal o połowę, z 14,85% do 7,76%[308]. Jest to związane głównie z nową formą cyberprzestępstwa, jaką jest *cryptojacking*, czyli zachowanie polegające na produkowaniu kryptowalut głównie za pomocą przeglądarki Monero. Przykładem firmy specjalizującej się w tego typu działaniach jest firma Coinhive[309]. Gdy użytkownik komputera odwiedzi taką zainfekowaną stronę, moc obliczeniowa jego komputera zostaje przejęta na potrzeby kopania kryptowaluty. Im więcej czasu użytkownik spędza na takiej stronie, tym więcej cykli procesora może być zużyte na potrzeby cyberprzestępcy[310].

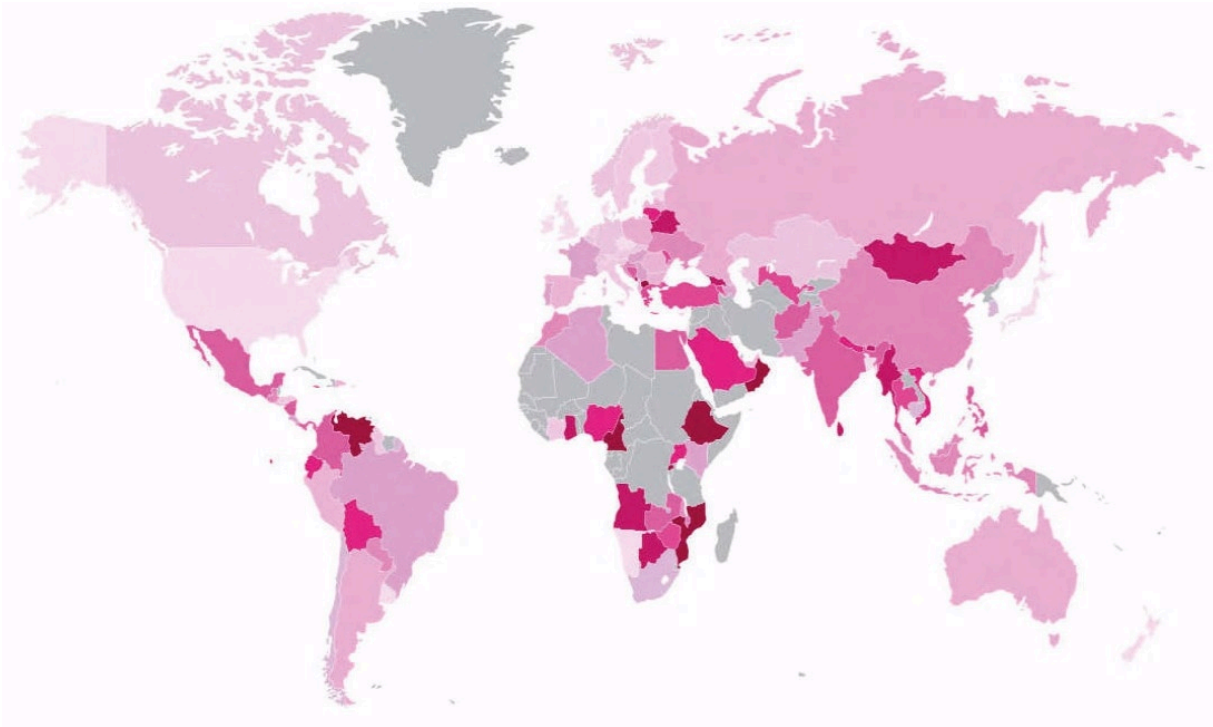


RYSUNEK 3.3
Ataki DDoS według rodzajów robaków w 2018 r.
Źródło: APWG Phishing Activity Trends Report 4th Quarter of 2017, http://www.apwg.org (dostęp: 27.05.2019).



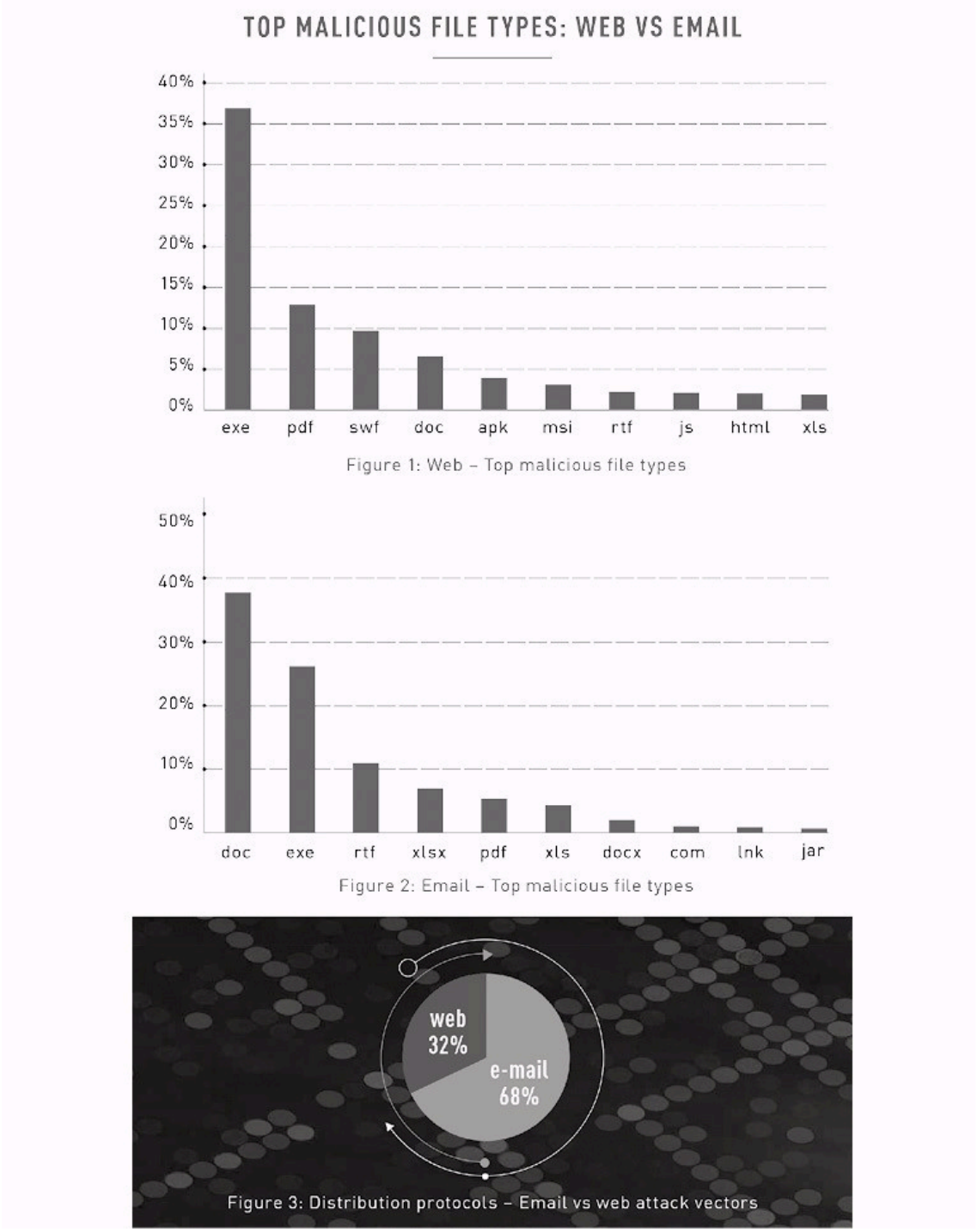
RYSUNEK 3.4 Liczba wykrytych szkodliwych pakietów instalacyjnych 2019–2020
Źródło: https://securelist.com/it-threat-evolution-q1-2020-statistics/96959/ (dostęp: 06.07.2020)

Na *rys. 3.5* zostały przedstawione główne obszary ataków cybernetycznych zaznaczone kolorami ciemnoróżowym i bordowym.



RYSUNEK 3.5
Kategorie cyberataku według regionu
Źródło: Cyber Security Report 2020, https://research.checkpoint.com (dostęp: 30.06.2020).

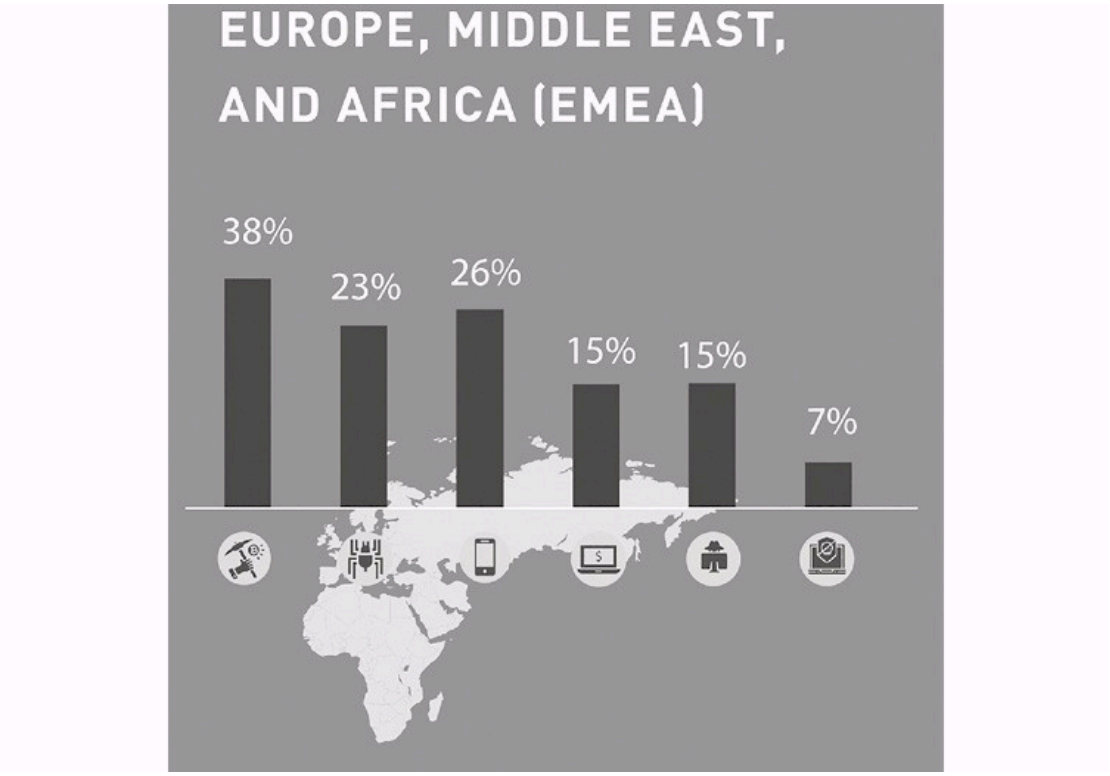
Cyberataki są przede wszystkim popełniane za pomocą poczty internetowej – 68%, na pierwszych trzech miejscach plasują się pliki typu .doc, .exe i .rtf. Natomiast 32% ataków jest popełnianych na stronach internetowych za pomocą plików .exe, .pdf i .swf.



RYSUNEK 3.6 10 głównych kategorii cyberataku
Źródło: Cyber Security Report 2020, https://research.checkpoint.com (dostęp: 30.06.2020).

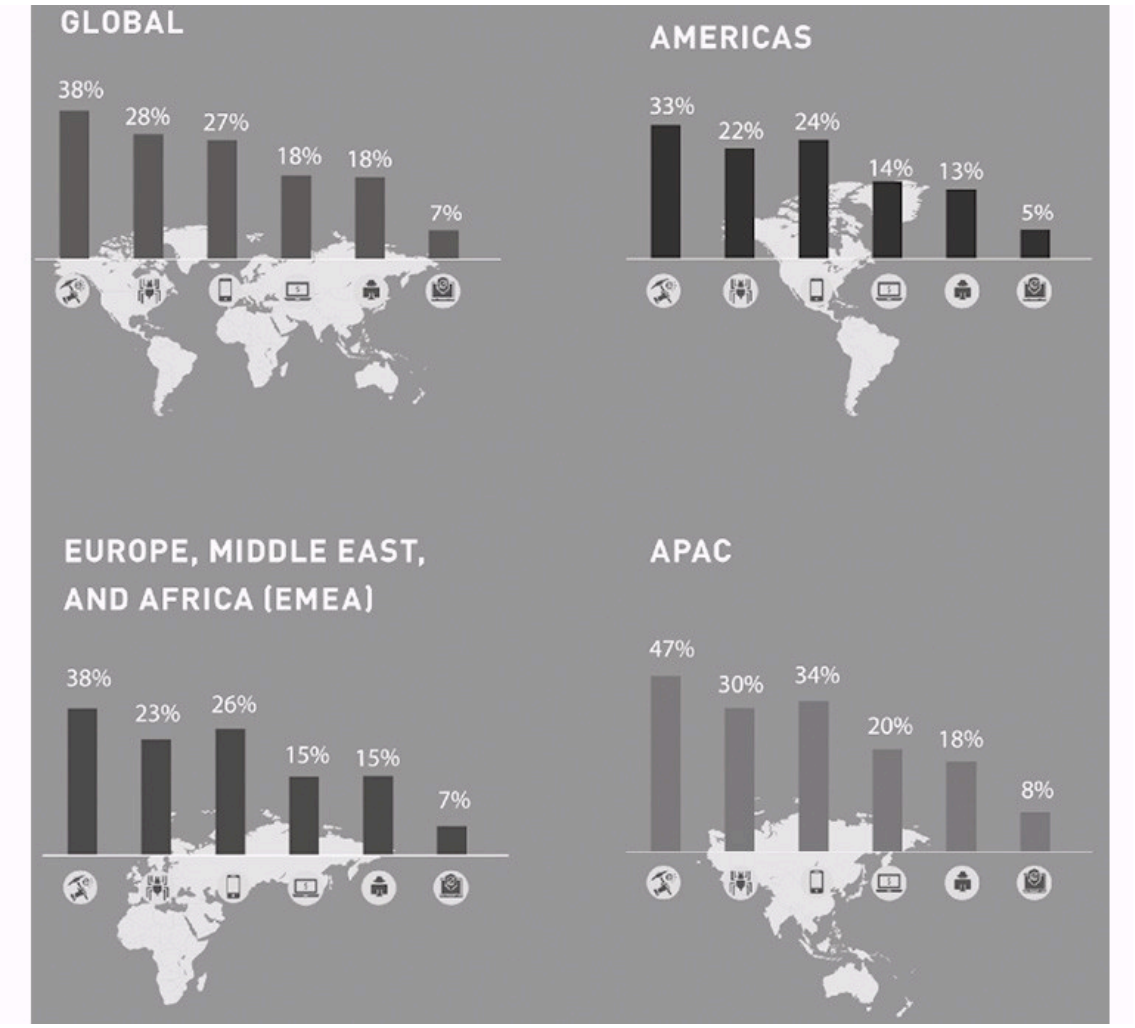
Głównymi źródłami cyberataku w Europie, podobnie jak na całym świecie, są: kryptowaluciarze, botnety, oszustwa bankowe, kradzież informacji komputerowych, ramsonware. Niektóre dane statystyczne różnią się natomiast liczbą popełnionych

przestępstw w naszym regionie względem całości świata, jednak nie odbiegają one w sposób znaczący od pozostałych kontynentów.



RYSUNEK 3.7
Źródła cyberataku w Europie, na Bliskim Wschodzie i w Afryce na tle świata
Źródło: Cyber Security Report 2020, https://research.checkpoint.com (dostęp: 30.06.2020).

Rozwój konwencjonalnego potencjału wojskowego wiąże się z reguły z bardzo wysokimi nakładami finansowymi, obejmującymi nie tylko szkolenie personelu, lecz także modernizację i utrzymanie sprzętu. Tymczasem narzędzia, które mogą zostać wykorzystane do ataku w środowisku teleinformatycznym, w tej perspektywie są prawie darmowe[311]. Wykorzystaniu cyberprzestrzeni sprzyja również fakt, że jak udowodniła operacja Orchard w 2007 r., środki tego typu mogą czasami zastępować lub uzupełniać konwencjonalne działania zbrojne[312].



RYSUNEK 3.8
Zestawienie źródeł cyberataku na świecie
Źródło: Cyber Security Report 2020, https://research.checkpoint.com (dostęp: 30.06.2020).

Cyberprzestrzeń oraz szybkość przeprowadzania ataków sprawiają, że prowadzenie działań obronnych jest utrudnione, a akcje ofensywne są relatywnie tanie i łatwe do przeprowadzenia. Wirtualność, jako cecha cyberprzestrzeni, jest tym wyraźniejsza, im większe jest uzależnienie społeczeństw od jej wykorzystania. Można tu bowiem zauważyć pewien paradoks, z jednej strony wykorzystanie technologii ICT we wszystkich sferach życia ludzkiego wiąże się z wieloma korzyściami, np. natury organizacyjnej, komunikacyjnej czy finansowej, z drugiej – zaawansowany technologicznie podmiot jest zdecydowanie bardziej wrażliwy na ataki teleinformatyczne. Ponadto, jak zauważył Fred Schreier[313], przestrzeń teleinformatyczna przez wielu jest postrzegana jako część wspólnego dziedzictwa ludzkości.

Czynnikiem zewnętrznym, który wywiera większy wpływ na środowisko bezpieczeństwa niż podziały w społeczności międzynarodowej, są procesy globalizacyjne. Globalizacja wydaje się już tak zaawansowana, że sieć różnych powiązań między państwami i społeczeństwami na świecie ma zbyt dużą gęstość, aby ulec dezintegracji czy znacznej redukcji. Nieuniknioną konsekwencją globalizacji jest erozja suwerenności państw, która dotyka każdego kraju, choć w zróżnicowanym stopniu. Wynika to z „odterytorialnienia" procesów społecznych oraz

pogłębiania się rozmaitych współzależności w skali globalnej lub międzynarodowej, w każdej dziedzinie życia społecznego. Proces ten dokonuje się stopniowo, jest jednak równie trwały jak globalizacja, wpływając w ten sposób na porządek i środowisko międzynarodowe[314].

Procesy globalizacji, zwłaszcza oddziałujące na sferę społeczno-ekonomiczną, tworzą nowe zagrożenia bezpieczeństwa. Ma również znaczenie fakt, że część zjawisk kryzysogennych toczy się poza jej terytorium. Wprost oddziałują one na wewnętrzną sytuację państw europejskich oraz społeczność europejską. W opinii znacznych części społeczeństw utrzymanie gwarancji zatrudnienia i adekwatnej liczby miejsc pracy, odpowiedniego poziomu bezpieczeństwa socjalnego czy tożsamości kulturowej powinno stać się priorytetem państwa.

3.2.2. UWARUNKOWANIA WEWNĘTRZNE

Spośród wszystkich koncepcji można wyodrębnić dwa nurty rozważań teoretycznych. Pierwszy z nich dotyczy podmiotu integracji, czyli kształtu ustrojowego europejskiej wspólnoty bezpieczeństwa. W nurcie drugim próbowano określić, jakie funkcje ta wspólnota powinna wypełniać. Dzięki temu ukształtowała się interesująca dziedzina badawcza nazwana teorią ról, która wypracowała własną metodologię, szczególnie w odniesieniu do Unii Europejskiej. Dla przykładu, Ryszard Zięba[315] uznał, że Unia Europejska pod koniec XX w. znalazła się w gronie najważniejszych uczestników stosunków międzynarodowych. Wskazał również jej cztery istotne role: lidera zrównoważonego rozwoju gospodarczego oraz wzorca pomyślnej i kompleksowej integracji, największego udziałowca w handlu światowym (w 2003 r. – AC), dostarczyciela największej pomocy rozwojowej, donatora największej pomocy humanitarnej. Spełnianie tych ról doprowadziło do uzyskania przez UE zasłużonego autorytetu. W sferze politycznej R. Zięba zwracał uwagę na „rolę aktywnego aktora dyplomatycznego", akcentując jednocześnie, że ta rola nie zawsze jest jednoznacznie akceptowana.

Stale rosnący wpływ technologii teleinformatycznych na rozwój społeczno-gospodarczy państw członkowskich Unii Europejskiej oraz wzrost ich wykorzystania sprawia, że obecnie oferowane produkty i usługi są coraz bardziej uzależnione od zapewnienia cyberbezpieczeństwa. Rozbudowana architektura systemów teleinformatycznych, w tym operacje na dużych zasobach danych, służy rozwojowi komunikacji, handlu, transportu i stanowią podstawę funkcjonowania usług kluczowych, cyfrowych i świadczonych przez administrację publiczną. Niestety możliwości, jakie oferują nowoczesne technologie cyfrowe, są też wykorzystywane w celu stosowania praktyk nieuczciwej konkurencji, przerywania ciągłości działania usług wybranych usług (w celu chuligańskim czy też osłabienia pozycji konkurencyjnej danego podmiotu), popełniania przestępstw z wykorzystaniem Internetu bądź prowadzenia działań o charakterze terrorystycznym[316].

Należy zbadać, jakie czynniki determinują rozumienie rozwoju społeczno-gospodarczego w odniesieniu do Unii Europejskiej. Podmiotem sprawczym, wywołującym zmianę w sposobie rozumienia tego zagadnienia, może być struktura państwowa lub międzynarodowa (np. UE), społeczeństwo (grupa społeczna) lub jednostka ludzka bądź siły natury. Założono, że istnieją pewne przyczyny, uwarunkowania, które oddziałują na sposób rozumienia rozwoju społeczno-gospodarczego w warunkach UE, i nazwano je czynnikami[317].

Wyodrębniono wiele czynników, przyjmując takie kryteria, jak czasowe, przestrzenne, strukturalne oraz dynamiki i intensywności oddziaływań[318]. Przyjmując kryterium przedmiotowe, można wyłonić te czynniki, które są związane ze sferą ustrojową i polityczną państw (czynnik polityczno-prawny), gospodarczą i społeczną, lecz także z ochroną środowiska naturalnego, sferą kulturową, kwestiami demograficznymi i przestrzennymi, czyli

zagadnieniami, które wpisują się w koncepcję szeroko pojmowanego (zrównoważonego) rozwoju społecznego. Biorąc pod uwagę kryterium czasowe, można te czynniki rozpatrywać pod kątem ich obowiązywania w czasie (historycznie, aktualnie i potencjalnie). Uwzględniając natomiast kryterium przestrzenne (zasięgu, terytorialne), nie można zapomnieć także o tym, że poza wymiarem wewnętrznym (państwem) w świecie oplecionym siecią wzajemnych powiązań szczególnego znaczenia nabiera wymiar zewnętrzny (czynnik międzynarodowy, zewnętrzny)[319].

Rozpatrując czynniki według kryterium strukturalnego, czyli pod kątem ich subiektywności, obiektywności, można przyporządkować większość z wymienionych czynników do sfery czynników generowanych przez człowieka, czynnik ekologiczny, traktując jako naturalny. Czynniki te mają charakter obiektywny. Z kolei, badając dynamikę i intensywność oddziaływania, można je podzielić na te, które wpływają bezpośrednio (polityczno-prawny, gospodarczy, społeczny, ekologiczny, kulturowy, demograficzny, przestrzenny) oraz pośrednio (zewnętrzny)[320]. Należy także zwrócić uwagę na wiele uwarunkowań wyjściowych dla danego państwa (np. położenie geograficzne, historię itp.) bądź takie czynniki, jak osobowościowe, czyli osobowość i charyzma głowy państwa itp., personalne (kadrowy), lecz także technologiczne, naukowe i komunikacyjne. Czynniki, które determinują pojmowanie rozwoju społeczno-gospodarczego w UE, zebrano w tabeli 3. Z jednej strony przedstawiono w niej zestawienie wyselekcjonowanych czynników, które uwarunkowują pojmowanie rozwoju społeczno-gospodarczego w odniesieniu do UE, z drugiej – ukazano zależności, które między poszczególnymi czynnikami zachodzą. Może być przydatna do kompleksowego badania czynników i zależności zachodzących w UE, przy czym należy podkreślić, że do jej opracowania wykorzystano założenia analizy czynnikowej. Proponowane zestawienie czynników ma charakter otwarty i może (powinno) być uzupełniane o inne czynniki, zależności w miarę ewoluowania Unii Europejskiej i jej otoczenia.

TABELA 3.3. Czynniki i zależności rozwoju społeczno-gospodarczego Unii Europejskiej

Czynniki	Polityczno-prawne	Społeczne	Gospodarcze	Ekologiczne	Przestrzenne	Demograficzne	Kulturowe
Polityczno-prawne	pp – pp	pp – s	pp – g	pp – e	pp – prz	pp – d	pp – k
Społeczne	s – pp	s – s	s – g	s – e	s – prz	s – d	s – k
Gospodarcze	g – pp	g – s	g – g	g – e	g – prz	g – d	g – k
Ekologiczne	e – pp	e – s	e – g	e – e	e – prz	e – d	e – k
Przestrzenne	prz – pp	prz – s	prz – g	prz – e	prz – prz	prz – d	prz – k
Demograficzne	d – pp	d – s	d – g	d – e	d – prz	d – d	d – k
Kulturowe	k – pp	k – s	k – g	k – e	k – prz	k – d	k – k

Legenda: pp – polityczno-prawne, s – społeczne, g – gospodarcze, e – ekologiczne, prz – przestrzenne, d – demograficzne, k – kulturowe

Źródło: opracowanie własne na podstawie: A. Bodnar, W. Szczepański, *Czynniki ewolucji współczesnych stosunków międzynarodowych*, Warszawa 1979, s. 14.

Wykorzystanie analizy czynnikowej do badań różnych zagadnień z zakresu nauk społecznych było rozpowszechnione zwłaszcza w latach siedemdziesiątych i osiemdziesiątych XX w. Metoda ta ma niewątpliwie tę zaletę, że akcentuje dynamikę i ewolucję rozważanego zjawiska, dając możliwość prognozowania kierunków jego rozwoju. Wskazuje zarówno na czynniki (uwarunkowania) danego zagadnienia, jak i na występujące zależności. Należy więc

przyjąć, że analiza czynnikowa może znaleźć zastosowanie do badania tak dynamicznego zagadnienia, jakim jest rozwój społeczno-gospodarczy Unii Europejskiej.

Cyberprzestrzeń jest także często określana jako nowego typu przestrzeń społeczna, w której funkcjonują ludzie. Jest to „wrażenie środowiska społecznego istniejącego wyłącznie w obszarze pewnego odwzorowania i komunikacji […]. Istnieje ono wyłącznie w przestrzeni komputerowej, rozproszonej w coraz bardziej złożonych i płynnych sieciowych powiązaniach”[321].

Rosnące zainteresowanie państw cyberprzestrzenią wiąże się również z szeroko pojętą sferą informacyjną. Przestrzeń teleinformatyczna posiada bowiem ogromny potencjał z perspektywy działalności propagandowej lub psychologicznej. Nowe technologie informacyjne i komunikacyjne mogą być skutecznie wykorzystane, np. do manipulowania opinią publiczną czy dezinformacji[322]. To ona obecnie decyduje o powstawaniu i kształtowaniu się społeczeństwa informacyjnego jako nowego systemu produkcyjnego (wytwórczego). Opierając się na rozwoju nowych technologii, wyznacza się nową rolę teleinformatyki i Internetu jako wielozadaniowego środka mogącego mieć zastosowanie w wielu obszarach z punktu widzenia gospodarki i społeczeństwa. Trzeba jednak pamiętać, że każde nowe działanie modernizacyjne czy innowacyjne ma swoje określone skutki społeczne, gospodarcze, ekonomiczne i kulturowe[323]. Doświadczenia w zakresie wprowadzania idei społeczeństwa informacyjnego pokazują, że obok zakładanych zjawisk pozytywnych występują zjawiska o wyraźnie negatywnym charakterze, odnoszące się zarówno do społeczeństwa, jak i indywidualnych ludzi[324]. Tymi zagrożeniami są nowe formy uwarstwienia społecznego, czyli podziału społeczeństwa pod kątem dostępu do informacji, wiedzy, wykształcenia, kwalifikacji. Historia pokazuje, że w przeszłości o pozycji i znaczeniu decydowało miejsce urodzenia, później kapitał, obecnie może to być umiejętność posługiwania się i wykorzystania technik teleinformacyjnych i dostępu do nich. Proces ten w czasach globalizacji może mieć znacznie większy zasięg, może obejmować nie tylko niektóre grupy społeczne, ale także całe społeczeństwa lub państwa[325].

Wrażliwym punktem prawidłowego funkcjonowania społeczeństw jest sprawne działanie infrastruktury telekomunikacyjnej. Na ataki cyberterrorystyczne są narażone technologie komputerowego przetwarzania danych, systemów zarówno telefonii komórkowej, jaki i stacjonarnej oraz satelitarnej. Winę za to po części ponoszą firmy, które produkują i wdrażają sprzęt telekomunikacyjny oraz oprogramowania. Systemy posiadające słabe strony nie są likwidowane, a umieszczane w utajnionej dokumentacji i fachowych artykułach z opisaną specyfiką tych słabości. Takie informacje szybko mogą trafić do niepowołanych osób. Największym zagrożeniem jest atak prowadzący do wyłączenia Internetu, jako całości. Skutek zablokowania serwerów DNS, których zadaniem jest tłumaczenie adresów IP, może być wszechogarniający. Atak uniemożliwiłby wymianę informacji, zawieranie kontraktów, a także realizację transakcji handlowych[326], [327].

Aktorów sceny cyberterrorystycznej znakomicie obrazuje schemat przedstawiony przez Thomasa R. Mockatisa[328], który wymienia kryminalne organizacje pełniące funkcję ubezpieczającą działania cyberterrorystyczne oraz państwa posługujące się terrorem i go wspomagające, wśród których ogromną rolę odgrywają grupy cyberterrorystyczne. Osoby, które mogą dokonać aktów cyberterrorystycznych, stanowią grupę działaczy różnych organizacji typową dla XXI w. W opinii specjalistów można wśród nich wyróżnić fanatyków religijnych, ortodoksyjnych działaczy New Age[329], separatystów i rewolucjonistów etniczno-narodowościowych oraz innego rodzaju ekstremistów[330]. Wśród fanów religijnych (szczególnie islamskich) w wielu przypadkach zauważa się, że metody cyberterrorystyczne nie są przez

nich stosowane. Przywódcy często nie znają się lub nie rozumieją nowoczesnych technologii, ponadto nie posiadają przygotowanej technologicznie i zaangażowanej ideowo kadry.

Inaczej jest w przypadku ortodoksyjnych działaczy New Age, wśród których można wyróżnić organizacje działające na rzecz praw zwierząt lub antyglobalistów. W ich szeregach są członkowie organizacji bardzo dobrze przygotowanych do roli cyberterrorystów, jednak ze względu na poglądy nie stosują cyberterroryzmu przeciw życiu ludzkiemu i wręcz wykluczają ofiary w ludziach. Bardzo groźną grupą (o różnym przygotowaniu specjalistycznym) są separatyści i rewolucjoniści etniczno-narodowościowi, którzy nie mają żadnych skrupułów w stosunku do obiektów ataku. W miarę postępu cywilizacyjnego na świecie mogą pojawić się innego typu ekstremiści.

TABELA 3.4. Uwarunkowania wewnętrzne UE w wymiarze polityczno-strategicznym

Wymiar						
CSDP – warstwa polityczna/strategiczna		**I**	**II**	**III**	**IV**	**V**
		Polityka/Strategia	**Cyberkultury**	**Umiejętności**	**Prawny i regulacyjny**	**Standardów, organizacji i możliwości**
Strategia globalna UE z 2016 r.	Poprawa reakcji na incydenty cybernetyczne w ramach WPBiO	√				
	Ochrona infrastruktury krytyczne wykorzystywana przez struktury WPBiO	√				
	Poprawa zarządzania kryzysowego w UE	√				
	Poprawa cyberobrony	√				
	Poprawa odporności systemów i procesów WPBiO	√				
	Promowanie zestawu zabezpieczeń dla WPBiO		√			
	Budowanie zaufania i pewności		√			
	Ochrona tożsamości i prywatności pracowników WPBiO			√		
	Rozważenie wykorzystania mediów społecznościowych w ramach WPBiO			√		
	Poprawa prawodawstwa dotyczącego cyberbezpieczeństwa				√	
	Koordynacja egzekwowania prawa w zakresie cyberprzestępczości				√	
	Działania rozwojowe i budowanie zaufania				√	

Wymiar						
CSDP – warstwa polityczna/strategiczna		**I**	**II**	**III**	**IV**	**V**
		Polityka/Strategia	**Cyberkultury**	**Umiejętności**	**Prawny i regulacyjny**	**Standardów, organizacji i możliwości**
	Promowanie współpracy międzynarodowej w kwestiach prawnych				√	
	Promowanie współpracy sektora publicznego i prywatnego				√	
	Opracowanie/przyjęcie wspólnych standardów					√
	Poprawa organizacji cyberobrony WPBiO					√
Strategia globalna UE z 2016 r.	Rozwijanie cyberstandardowych procedur operacyjnych zapewniających zgodność między reagowaniem na incydenty cywilne i wojskowe	√				
	Opracowanie zasad oceny ryzyka cybernetycznego infrastruktury krytycznej dla kwater głównych i misji WPBiO	√				
	Opracowanie zasad koordynacji wysiłków między strukturami cywilnymi i wojskowymi podczas cyberkryzysów	√				
	Cyberobrona jako zadanie operacyjne dla misji WPBiO i uwzględnianie kwestii cyberobrony w procesach planowania operacyjnego WPBiO	√				
	Dalszy rozwój współpracy między WPBiO i UE (np. ENISA, EC3) oraz sojusznikami strategicznymi (np. NATO) na poziomie operacyjnym	√				
	Promowanie współpracy między agencjami, organami i instytucjami UE w		√			

Wymiar						
CSDP – warstwa polityczna/strategiczna		**I**	**II**	**III**	**IV**	**V**
		Polityka/Strategia	**Cyberkultury**	**Umiejętności**	**Prawny i regulacyjny**	**Standardów, organizacji i możliwości**
	zakresie wymiany informacji					
	Promowanie kampanii w cyberprzestrzeni ukierunkowanych na struktury dowodzenia w ramach WPBiO		√			
	Opracowanie środków w celu ochrony prywatności pracowników WPBiO zgodnie z rozporządzeniem RODO		√			
Strategia globalna UE z 2016 r.	Opracowanie środków mających na celu ochronę tożsamości personelu WPBiO podczas misji		√			
	Opracowanie zasad korzystania z mediów społecznościowych dla pracowników WPBiO		√			
	Wykorzystanie mediów społecznościowych jako źródło OSINT dla misji WPBiO		√			
	Opracowanie ścieżek szkoleniowych związanych z cyberobowiązkami dla kwater głównych WPBiO			√		
	Poznanie możliwości edukacji i szkolenia w zakresie cyberobrony oraz synergie dla planistów operacyjnych WPBiO			√		
	Zintegrowanie cyber z istniejącymi ćwiczeniami operacyjnymi (planowanie, wykonanie, ocena, wyciągnięte wnioski)			√		
	Zastanowienie się nad udziałem w przyszłych ogólnoeuropejskich ćwiczeniach z zakresu			√		

Wymiar						
CSDP – warstwa polityczna/strategiczna		**I**	**II**	**III**	**IV**	**V**
		Polityka/Strategia	**Cyberkultury**	**Umiejętności**	**Prawny i regulacyjny**	**Standardów, organizacji i możliwości**
	bezpieczeństwa cybernetycznego (np. Cybereurope)					
	Zapewnienie wsparcia prawnego w zakresie opcji cyberobrony dowódcom/dyrektorom operacyjnym WPBiO				√	
	Stymulowanie świadomości personelu WPBiO na temat zagrożeń, a także w kontekście misji WPBiO				√	
Strategia globalna UE z 2016 r.	Ulepszenie ram regulacyjnych dotyczących współpracy między sektorem prywatnym a kwaterami głównymi WPBiO w zakresie świadczenia usług dotyczących bezpieczeństwa cybernetycznego				√	
	Opracowanie/przyjęcie określonych wymagań/standardów cyberbezpieczeństwa dla systemów wojskowych (c4isr) wykorzystywanych w misjach WPBiO					√
	Opracowanie obowiązków w zakresie stałej obrony w strukturze operacyjnej WPBiO					√
	Rozważenie możliwości oceny zagrożenia cybernetycznego					√
	Rozważenie możliwości oceny cyberodporności w WPBiO					√
	Integrowanie cyberprzestrzeni w ramach wspólnego obrazu operacyjnego misji WPBiO					√

Wymiar						
CSDP – warstwa polityczna/strategiczna		I	II	III	IV	V
		Polityka/Strategia	Cyberkultury	Umiejętności	Prawny i regulacyjny	Standardów, organizacji i możliwości
	Integrowanie cyberinteligencji ze sztuczną inteligencją					√

Źródło: opracowanie własne na podstawie *Cybersecurity in the EU Common Security and Defence Policy (CSDP) Challenges and risks for the EU*. Study, dok. RS/STOA/SER/16/214N, Brussels 2017, s. 49–52 oraz https://www.enisa.europa.eu/news/enisanews/standard-operational-procedures-to-manage-multinational-cyber crises-finalised-by-eu-efta-memberstates-and-enis (dostęp: 15.05.2020).

W wyniku występowania ogromnej skali cyberzagrożeń coraz częściej słychać opinie, że UE nie spełnia oczekiwań w dziedzinie cyberobrony. Ponadto państwa członkowskie wciąż rozwijały rozbieżne strategie cyberbezpieczeństwa oraz wyrażały odmienne poglądy na temat tego, jak podmioty państwowe oraz instytucje UE powinny przyczyniać się do odporności cybernetycznej na szczeblu europejskim. W rezultacie każdy obszar europejskiej strategii bezpieczeństwa cybernetycznego wydanej w 2013 r. znajdował się na innym etapie rozwoju.

Przechodząc do uwarunkowań wewnętrznych, planowane i podejmowane środki i działania będące częścią ram polityki UE w zakresie cyberobrony, ale także wykraczające poza te ramy powinny być spójne z pięcioma wymiarami wspomnianymi wcześniej w rozdziale 2.3.

Uwarunkowania wewnętrze UE są ściśle powiązane z odpowiednimi środkami wdrażanymi na poziomie operacyjnym. Taktyczna warstwa w WPBiO stanowi pierwszą linię obszarów cyberoperacji. Często warstwa ta pod względem ludzkim nie ma zasobów i zdolności lub działa w niesprzyjających warunkach również poza granicami UE. Dlatego bardzo ważne jest to, aby móc zbudować dojrzałą cyberprzestrzeń, która jest elastyczna, skalowalna i, co najważniejsze, cybergodna. Ważne jest również, aby zdolność ta była w stanie przekazywać wiarygodne informacje w niezawodny sposób do warstwy operacyjnej, jeśli chodzi o cyberzagrożenia w cyberoperacjach. Dlatego potrzebna jest poprawa współpracy w zakresie wymiany informacji i najlepszych praktyk między wojskowymi a cywilnymi zespołami WPBiO, prowadzenie kampanii uświadamiających skierowanych zarówno do pracowników WPBiO, jak i do obywateli UE, mających na celu zwiększenie wiedzy i świadomości na temat ochrony danych, prywatności i tożsamości, za pośrednictwem agencji takich jak ENISA.

* * *

Przeprowadzone badania prowadzą do kilku wniosków. Po pierwsze, istotę analizy czynnikowej charakteryzują zidentyfikowane przez badacza czynniki warunkujące badany problem, zależności między podmiotami w odniesieniu do tego problemu oraz możliwość przewidzenia kierunków ewolucji danego zjawiska. Jest to zatem metoda adekwatna do badania zjawisk o dynamicznym, zmiennym charakterze.

Po drugie, rozwój społeczny jest kategorią szerszą niż rozwój (wzrost) gospodarczy, ponieważ obejmuje czynnik ludzki. Jest to kategoria zmienna, którą należy rozpatrywać w ujęciu procesualnym. Jej dynamizm uzasadnia przydatność badania tego zagadnienia w odniesieniu do UE za pomocą analizy czynnikowej.

Po trzecie, przyjmując dane kryteria, można wyłonić wiele czynników przydatnych do badania rozwoju społeczno-gospodarczego UE. Pomocne jest tu przede wszystkim kryterium przedmiotowe, zgodnie z którym można wyłonić czynniki: polityczno-prawny, gospodarczy,

społeczny, ekologiczny, kulturowy, demograficzny, przestrzenny, które ponadto wpisują się w koncepcję szeroko pojmowanego zrównoważonego rozwoju.

Przedstawione wnioski potwierdzają zatem założoną na wstępie tezę badawczą. Analiza czynnikowa, będąc metodą badawczą z zakresu nauk społecznych, może być wykorzystywana do badania zagadnienia takiego, jak rozwój społeczno-gospodarczy w warunkach Unii Europejskiej.

Z zaprezentowanych rozważań wynika, że bezpieczeństwo jest wartością, ale i dynamicznym procesem podlegającym ewolucji w warunkach zmiany rzeczywistości społecznej. Zagrożenia stwarzają najczęściej państwa lub podmioty niepaństwowe o stwierdzonych wrogich zamiarach wobec innych państw bądź organizacji, dysponujące środkami ich realizacji. Zagrożenia w sferze teleinformatycznej są coraz trudniejsze do identyfikacji, dążąc do dezorganizacji kluczowych systemów informacyjnych instytucji rządowych, elementów infrastruktury krytycznej, w tym baz danych. Czynnikami sprzyjającymi powstawaniu tego typu zagrożeń są niskie koszty przygotowania operacji oraz ogromna skala zniszczeń. Cechą charakterystyczną tych działań jest ich globalny zasięg.

Zagrożenia bezpieczeństwa społeczeństwa informacyjnego są realne, występują w codziennej rzeczywistości działania podmiotu, zatem rozpoznanie, osiągnięcie, utrzymanie i doskonalenie bezpieczeństwa informacyjnego staje się nieodzowne do zapewnienia przewagi konkurencyjnej organizacji, płynności finansowej, rentowności, pozostawania w zgodzie z literą prawa.

Działalność cyberterrorystów w sieci jest bardzo poważnym problemem, gdyż ich poczynania są ukryte. Z uwagi na łatwość maskowania tożsamości można mówić o relatywnej anonimowości atakujących, którzy bez obaw, że zostaną wykryci, przeprowadzają za pomocą sieci wrogie działania. Wynika stąd kolejny problem – skala potencjalnych strat, pod względem zarówno finansowym, jak i bezpieczeństwa, jest trudna do oszacowania[331].

Polityka cyberbezpieczeństwa UE jest reakcją na zaistniałe zagrożenie, jakim nie jest ochrona jakiegoś wspólnego dobra[332]. Dzisiaj niemal każda nielegalna działalność ma odzwierciedlenie w Internecie. Globalny charakter Internetu dał natomiast szansę ludziom na zmianę wymiaru komunikacji i aktywności życiowych. Cyberprzestrzeń jest obecnie postrzegana jako przestrzeń polityczno-społeczna, w której odbijają się te same problemy, co w świecie rzeczywistym. Cyberprzestępczość jest również odmianą przestępczości, wykorzystującą możliwości technik cyfrowych i środowiska sieci komputerowych.

Przyczyną powstania polityki cyberbezpieczeństwa jest również brak odpowiednich mechanizmów i regulacji w tym zakresie, dlatego mamy do czynienia z procesem instytucjonalizacji. Cyberprzestępczość od klasycznej przestępczości odróżnia przede wszystkim wirtualność[333].

Nową, bardzo niebezpieczną zmianę w cyberterroryzmie wyznacza pojawienie się tzw. najemników. Tendencja wykorzystywania znawców zaawansowanych technologii w przestępczych działaniach komputerowych[334] się nasila. Zdaniem A. Rathmella[335] organizacje terrorystyczne posługujące się nowymi technikami można podzielić na trzy kategorie:

- kategoria I – obejmuje nowe techniki używane przez terrorystów do prowadzenia tradycyjnej działalności, Internet wykorzystuje się tutaj do zbierania informacji, komunikacji, zdobywania środków finansowych i komunikacyjnych;
- kategoria II – wykorzystywane są stare techniki do nowej działalności, używana jest siła fizyczna, która ma na celu zniszczenie systemu informacyjnego,
- kategoria III – używa się w niej nowe techniki do nowych działań, to atak w cyberprzestrzeni na system informacyjny[336].

Można również zauważyć, że organizacje ekstremistyczne (głównie islamskie) w celu wsparcia swoich działań i przeprowadzania ofensywnych ataków coraz częściej budują sieci hakerskie. Obecnie można wyróżnić trzy poziomy zagrożenia związanego z cyberterroryzmem[337]. Pierwszym z nich jest tzw. *simple-unstructured*, który polega na dokonaniu przez cyberterrorystów prostych włamań do indywidualnych systemów informacyjnych przez wykorzystanie narzędzi internetowych skonstruowanych przez inną osobę. Drugim poziomem zagrożenia jest tzw. *advanced-structured*. Na tym poziomie cyberterroryści dokonują bardziej skomplikowanych ataków przeciw złożonym sieciom komputerowym i systemom. Mają możliwość tworzenia lub modyfikowania własnych narzędzi, które służą do atakowania w cyberprzestrzeni, posiadają zdolność analizy celów, które będą przedmiotem ataku, a także dowodzenia, kontroli i uczenia się nowych metod atakowania. Ostatnim, najpoważniejszym poziomem zagrożenia jest tzw. *complex-coordinated*. Cyberterroryści dokonują tu skoordynowanych ataków w celu totalnej destrukcji zintegrowanego systemu obronnego, mają możliwość tworzenia skomplikowanych narzędzi, które służą do niszczenia celów w cyberprzestrzeni, a także analizę obiektów będących przedmiotem ataku. Mogą dowodzić, kontrolować i samodoskonalić się.

* * *

W okresie rozwoju cyberterroryzmu ochrona cyberprzestrzeni to niezwykle ważne, ale zarazem trudne i złożone przedsięwzięcie. Wymaga zaangażowania znacznych potencjałów państw i organizacji w wymiarze międzynarodowym i krajowym oraz stosowania nowych rozwiązań technik i technologii skutecznie przeciwdziałających temu niezwykle szkodliwemu i niebezpiecznemu zagrożeniu. Analiza literatury przedmiotu dotycząca zagrożeń i metod przeciwdziałania zagrożeniom oraz obserwacje działań państw i różnego rodzaju organizacji wskazują, że proces ten, poza działaniami specjalistycznymi, powinien być wspierany metodami stosowanymi w obszarze bezpieczeństwa informacji i systemów teleinformatycznych oraz telekomunikacyjnych zarówno publicznych, jak i mających zastosowania specjalne w obszarze bezpieczeństwa państwa i zarządzania kryzysowego.

Uogólniając prezentowane treści, można sprecyzować następujące wnioski:

- cyberterroryzm to szczególne zagrożenie cywilizacji, społeczeństwa informacyjnego, bezpieczeństwa narodowego i obywateli, które wymaga przeciwdziałania i zdecydowanego zwalczania;
- ochrona cyberprzestrzeni jest jednym z podstawowych zadań administracji państwowej i podmiotów odpowiedzialnych za tego typu działania, jest zadaniem priorytetowym dla organizacji międzynarodowych i różnego rodzaju kooperacji w skali globalnej i regionalnej, przykładem są działania administracji Unii Europejskiej, która przypisuje szczególne znaczenie zwalczaniu cyberterroryzmu i ochrony cyberprzestrzeni oraz jej funkcjonowania;
- formy cyberterroryzmu, rodzaje ataków i metody ich prowadzenia są znane oraz powtarzające się, przygotowanie na wymaganym poziomie zasobów osobowych i materialnych państwa oraz różnych organizacji umożliwia skuteczną ochronę cyberprzestrzeni;
- metody i sposoby zapewnienia bezpieczeństwa informacji i systemów teleinformatycznych organizacji powinny być stosowane w sposób kompleksowy, taka praktyka działania wychodzi naprzeciw potrzebom ochrony cyberprzestrzeni, terroru;
- obecna polityka cyberbezpieczeństwa Unii Europejskiej powinna zmierzać w kierunku zapewnienia bezpieczeństwa systemów informacyjnych, które jest istotą bezpieczeństwa informacyjnego.

Ze względu na swoje znaczenie bezpieczeństwo informacyjne należy rozpatrywać w obszarach bezpieczeństwa organizacji i instytucji oraz obywatela. Wcześniej o kształcie obiegu informacji decydowała struktura społeczna. Obecnie nie tylko ona ma znaczenie, ponieważ w systemie informacyjnym wywierającym wpływa na społeczeństwo oprócz państwa występują środki masowego przekazu i cyberprzestrzeń.

4

PRAWNE STANDARDY CYBERBEZPIECZEŃSTWA UNII EUROPEJSKIEJ

Czwarty rozdział stanowi kontynuację rozważań rozpoczętych w rozdziale trzecim. Ponieważ prawo ochrony cyberprzestrzeni Unii Europejskiej należy traktować jako szczególny przypadek prawa międzynarodowego, zostanie pokazany wpływ prawa międzynarodowego, obowiązującego przed powstaniem Unii Europejskiej, na obecny kształt prawa unijnego. Zostanie również przeprowadzona analiza procesu uwspólnotowienia polityki cyberbezpieczeństwa Unii Europejskiej na podstawie przyjętych rozwiązań prawnych. Analiza podstaw prawnych pozwoli na wykazanie zależności polityki cyberbezpieczeństwa od poziomu integracji państw członkowskich oraz związku funkcjonalnego zachodzącego między harmonizacją przepisów prawa państwowego z prawem unijnym w dziedzinie bezpieczeństwa, ponieważ proces ten nie został zakończony.

W pierwszej części zostaną poddane analizie międzynarodowe standardy zwalczania cyberterroryzmu zawarte przez Radę Europy, ONZ czy Interpol w konwencjach międzynarodowych. Zostanie także omówiony ich instytucjonalny wymiar zwalczania cyberprzestępczości w prawie międzynarodowym. W drugiej części rozdziału zostaną przedstawione zagadnienia prawne polityki ochrony cyberprzestrzeni Unii Europejskiej z podziałem na prawo

pierwotne i wtórne. Na koniec zostanie przedyskutowany instytucjonalny wymiar zwalczania cyberprzestępczości w prawie Unii Europejskiej.

Jedną z przyczyn cyberataków jest brak właściwych regulacji i mechanizmów w obszarze ochrony cyberprzestrzeni. Stworzenie określonych ram prawnych w tym obszarze stanowi podstawowe wyzwanie polityki ochrony cyberprzestrzeni dla dalszego rozwoju UE i państw członkowskich.

4.1
MIĘDZYNARODOWE NORMY PRAWNE W ZAKRESIE ZWALCZANIA CYBERTERRORYZMU

4.1.1. RADA EUROPY WOBEC CYBERPRZESTĘPCZOŚCI

Pod koniec XX w. wraz z postępującą komputeryzacją i usieciowieniem społeczeństwa, a także narastaniem zjawiska cyberprzestępczości coraz ważniejsza stała się potrzeba utworzenia i uporządkowania systemu środków prawnych służących do zwalczania nowych rodzajów zagrożeń. Już w latach dziewięćdziesiątych XX w. takie działania zaczęto podejmować w ramach Rady Europy, Unii Europejskiej, OECD oraz ONZ[338]. Zainteresowanie tymi zagadnieniami zaowocowało wypracowaniem ramowych zasad zwalczania różnych form cyberprzestępczości w prawie międzynarodowym i unijnym. W pierwszej kolejności takie zasady zostały wypracowane na forum Rady Europy[339], której działalność stała się podstawą prac legislacyjnych podejmowanych przez organy Unii Europejskiej.

Jednym z ważniejszych aktów prawnych odnoszących się do problematyki zwalczania cyberprzestępczości jest *Konwencja Rady Europy o cyberprzestępczości*[340]. Jej uchwalenie uzasadniono koniecznością podjęcia zdecydowanych działań mających na celu

uwspólnienie zasad zwalczania i ścigania cyberprzestępców oraz wypracowanie procedur ich ekstradycji zarówno z państw o restrykcyjnej, jak i liberalnej polityce karnej. Takie incydenty były coraz bardziej popularne, dlatego też konieczna była międzynarodowa współpraca w celu efektywnego zwalczania tego zjawiska i przeciwdziałania mu, m.in. przez wymianę doświadczeń oraz unifikację przepisów proceduralnych.

Konwencja o cyberprzestępczości była pierwszą umową międzynarodową, która regulowała kwestię przestępczości w przestrzeni wirtualnej. Jej celem było zapewnienie ochrony użytkowników cyberprzestrzeni oraz bezpieczeństwa sieci m.in. poprzez zwalczanie pornografii dziecięcej oraz treści rasistowskich i ksenofobicznych w Internecie. W znacznym stopniu przyczyniła się do zharmonizowania i ujednolicenia terminologii stron umowy, określenia katalogu najpoważniejszych cyberprzestępstw oraz zakreślenia przepisów proceduralnych i jurysdykcyjnych[341].

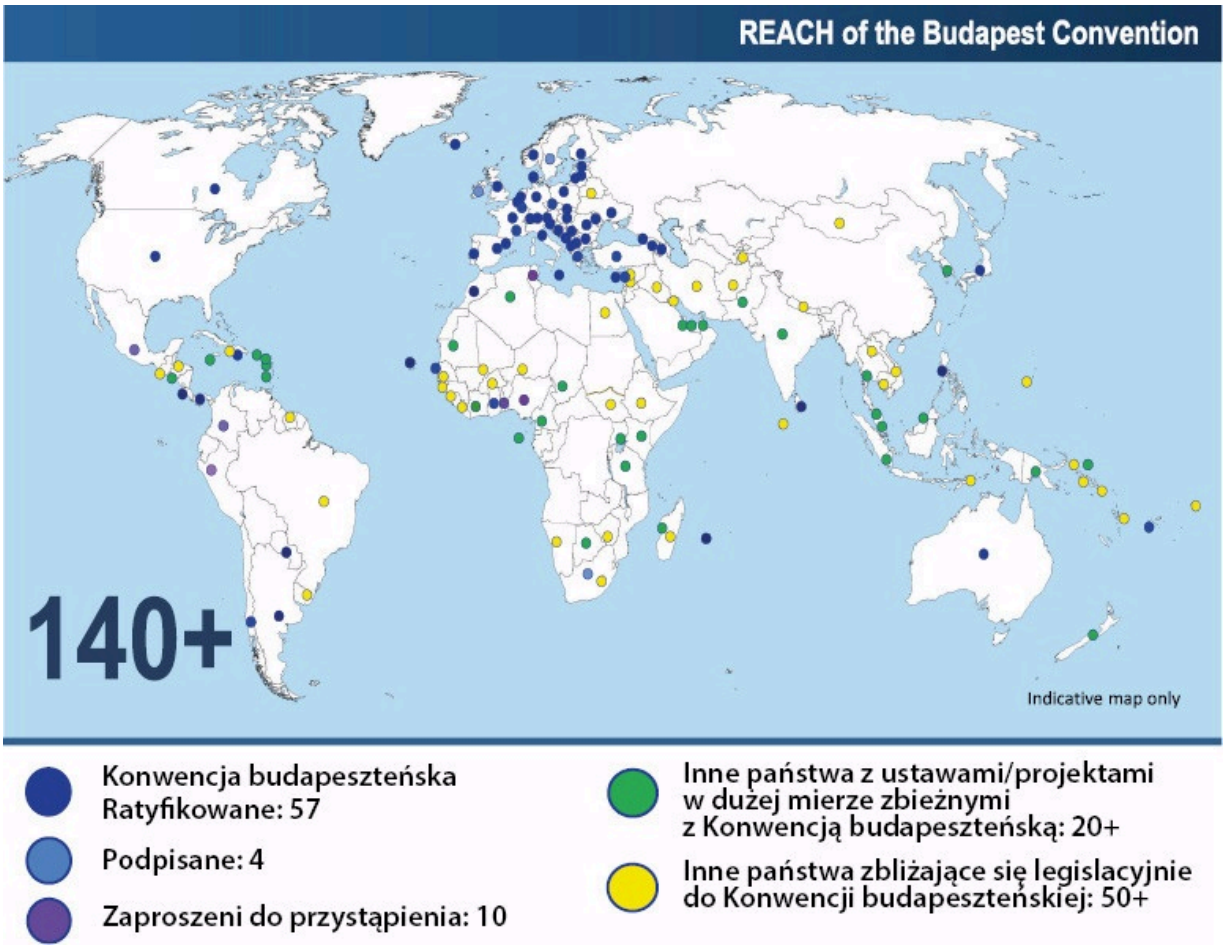
Przepisy materialnoprawne zawarte we wspomnianej konwencji nie mogą być stosowane bezpośrednio, ponieważ nie są wystarczająco precyzyjne i nie mają charakteru norm samowykonalnych[342]. Oznacza to, że państwa członkowskie mogą zdecydować się na kryminalizację innych czynów, które w ich ocenie powinny podlegać karze. Przepisy zawarte w tym dokumencie stanowią minimalny standard w zakresie penalizacji, „mogą być jednak stosowane pośrednio jako wskazówka przy wykładni przepisów prawa krajowego mających dokonać ich transpozycji”[343] w zakresie cyberprzestępstw.

Można zauważyć, że twórcy konwencji podzieli czyny na kilka kategorii. Pierwszą z nich stanowią przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów zawarte w art. 2–6 konwencji, tj. nielegalny dostęp do systemu informatycznego, nielegalne przechwytywanie danych, naruszenie integralności danych, naruszenie integralności systemu, niewłaściwe użycie urządzeń. Drugą tworzą przestępstwa komputerowe stypizowane w art. 7–8 konwencji, czyli oszustwo i

fałszerstwo komputerowe. Trzecia kategoria to przestępstwa związane z pornografią dziecięcą ujęte w art. 9.

Zgodnie z art. 10 konwencji państwa członkowskie powinny uznać za przestępstwa działania związane z naruszeniem praw autorskich i praw pokrewnych polegające na umyślnym i bezprawnym dostępie do całości lub części systemu informatycznego, przechwytywaniu za pomocą urządzeń technicznych niepublicznej transmisji danych informatycznych, niszczeniu, wykasowywaniu, uszkadzaniu, dokonywaniu zmian, spowodowaniu poważnych szkód oraz wprowadzaniu, transmisji, niszczeniu, wykasowywaniu lub dokonywaniu zmian w danych, które w rezultacie powodują poważne naruszenie integralności systemu informatycznego oraz użycie urządzeń, udostępnianie haseł, programów komputerowych czy też innych informacji, w celu popełnienia wspomnianych przestępstw (tzw. niewłaściwe użycie)[344]. Za przestępstwo należy uznać także oszustwa i fałszerstwa komputerowe, przestępstwa związane z pornografią dziecięcą, naruszeniem praw autorskich i praw pokrewnych. Przewidziano także odpowiedzialność karną za usiłowanie, pomocnictwo i podżeganie. Dodatkowo zdefiniowano zasady odpowiedzialności osób prawnych za wymienione przestępstwa[345].

Zgodnie z art. 16 strony *Konwencji Rady Europy o cyberprzestępczości* zostały zobowiązane do przyjęcia środków prawnych umożliwiających nakazanie lub uzyskanie niezwłocznego zabezpieczenia danych informatycznych, w tym także danych dotyczących ruchu, szczególnie gdy istnieje ryzyko ich utraty lub modyfikacji. Podkreślono, że przyjęte środki prawne powinny również obejmować uprawnienia do zajęcia i zabezpieczenia systemu informatycznego lub jego części, wykonania i zachowania kopii całości bądź części danych, uczynienia danych niedostępnymi lub ich usunięcia z systemu. Uprawnione organy powinny mieć dodatkowo prawo do niezwłocznego rozszerzenia poszukiwań na inny system, jeżeli istnieje uzasadnione przypuszczenie, że poszukiwane dane są przechowywane w innym niż początkowo założono systemie informatycznym (art. 17 konwencji)[346].



RYSUNEK 4.1
Mapa świata dotycząca obowiązywania norm *Konwencji RE o cyberprzestępczości*

Źródło: *Raport Analysis of the Council of Europe*, http://coe.int/cybercrime z kwietnia 2018 r., s. 3.

Protokół dodatkowy do *Konwencji Rady Europy o cyberprzestępczości* dotyczący kryminalizacji działań o charakterze rasistowskim i ksenofobicznym popełnianych przy użyciu systemów komputerowych został sporządzony 28 stycznia 2003 r. w Strasburgu[347]. Przyczyną jego sporządzenia była próba ujednolicenia systemu prawa międzynarodowego, który mógłby zapewnić odpowiednie środki prawne reagowania na propagandę o charakterze rasistowskim i ksenofobicznym rozprzestrzenianą za pomocą cyberprzestrzeni. Ma on stanowić równowagę między

swobodą wyrażania opinii a efektywną walką z atakami o charakterze rasistowskim i ksenofobicznym.

Strony umowy w art. 1 ust. 1 protokołu dodatkowego uznały za materiały rasistowskie i ksenofobiczne „każdy materiał pisemny, każdy wizerunek lub każde inne wyrażenie myśli lub teorii, które nawołują, popierają lub podżegają do nienawiści, dyskryminacji lub przemocy przeciw jakiejkolwiek osobie lub grupie osób, ze względu na rasę, kolor, pochodzenie narodowe lub etniczne, jak również religię, jeżeli wykorzystywana jest ona jako pretekst dla któregokolwiek z tych czynników".

Państwa strony na mocy protokołu dodatkowego zobowiązały się do penalizacji następującej kategorii czynów:

- rozpowszechniania materiałów o charakterze rasistowskim lub ksenofobicznym w systemie komputerowym rozumiane jako umyślna i bezprawna dystrybucja lub publiczne udostępnianie materiałów rasistowskich i ksenofobicznych w systemie komputerowym, strony umowy mogą jednak zastrzec, że nie będą stosować wskazanej regulacji w swoim prawie krajowym, jeżeli byłoby to sprzeczne z wewnętrznymi przepisami zapewniającymi swobodę wyrażania opinii lub jeżeli czyn nawołuje, popiera lub podżega do dyskryminacji, która jednak nie jest związana z przemocą lub nienawiścią (art. 3);
- kierowania gróźb o podłożu rasistowskim lub ksenofobicznym, czyli czyn polegający na grożeniu za pomocą systemu komputerowego popełnieniem poważnego przestępstwa na szkodę określonej osoby lub grupy osób z powodu jej/ich przynależności do grupy wyodrębnionej ze względu na rasę, kolor, pochodzenie narodowe lub etniczne albo wyznanie (art. 4);
- publicznego znieważania ze względów rasistowskich lub ksenofobicznych rozumianego jako publiczna zniewaga popełniona przy użyciu systemu komputerowego przeciwko osobie lub grupie osób z powodu jej/ich przynależności do grupy wyodrębnionej ze względu na rasę, kolor, pochodzenie narodowe lub etniczne albo wyznanie (art. 5);

- zaprzeczania, poważnego umniejszania znaczenia, akceptacji lub usprawiedliwiania zbrodni ludobójstwa oraz zbrodni przeciwko ludzkości zdefiniowane przez akty prawa międzynarodowego oraz przez wiążące decyzje międzynarodowych sądów karnych (art. 6).

Protokół dodatkowy przewiduje, że pomocnictwo i podżeganie do popełnienia któregokolwiek z wymienionych czynów również jest karalne.

Konwencja o cyberprzestępczości jest najważniejszym, ale nie jedynym aktem prawnym wypracowanym przez Radę Europy, a dotyczącym zwalczania zagrożeń w cyberprzestrzeni. Poważnym niebezpieczeństwem związanym z łatwością komunikowania się za pośrednictwem Internetu i innych sieci komputerowych jest możliwość wykorzystania sieci w celu rozpowszechniania informacji zakazanych przez prawo. Przykładem zwrócenia uwagi na ten właśnie problem może być *Konwencja o ochronie dzieci przed wykorzystaniem seksualnym* z 2007 r.[348] Jej podstawowym celem jest ustanowienie specjalnego mechanizmu monitoringu działającego na zasadzie współpracy krajowej i międzynarodowej. Ma on zapobiegać wykorzystywaniu seksualnemu dzieci i zwalczać ten proceder, w związku z czym konwencja ta stanowi podstawę prawną ochrony praw dzieci będących ofiarami wykorzystywania seksualnego[349].

Wzrastające do niepokojących rozmiarów wykorzystanie seksualne i niegodziwe traktowanie dzieci w celach seksualnych, zwłaszcza coraz szersze stosowanie do tego celu technologii informacyjnych i komunikacyjnych, spowodowało zawarcie w przepisach konwencji stosownych regulacji. W myśl art. 4 konwencji każda ze stron została zobowiązana do podjęcia stosownych środków w celu zapobieżenia wszelkim formom wykorzystywania seksualnego i niegodziwego traktowania dzieci w celach seksualnych oraz do ochrony dzieci. Poszczególne typy przestępstw zostały ujęte w art. 18–22 tego dokumentu. W art. 20 zawarto natomiast postanowienie, w myśl którego państwa powinny podjąć działania w celu spenalizowania przestępstw dotyczących pornografii dziecięcej, w tym produkowania, oferowania i udostępniania, dystrybuowania lub

przesyłania, pozyskiwania, posiadania pornografii dziecięcej, ale także świadomego uzyskiwania dostępu do pornografii dziecięcej za pośrednictwem technologii informacyjnych i komunikacyjnych.

Początki prawnej ochrony danych osobowych w Europie rozpoczęły działania Rady Europy. Już w 1968 r. Komitet Ministrów Rady Europy rozpoczął prace zmierzające do „przyjęcia kompleksowego aktu prawnego odnoszącego się do ochrony danych w państwach członkowskich”[350], które doprowadziły do przyjęcia tekstu konwencji nr 108. Była to pierwsza umowa międzynarodowa w Europie dotycząca tematyki przetwarzania danych osobowych, określająca minimalne standardy ich ochrony[351]. Konwencja ta „była i pozostanie jedynym prawnie wiążącym międzynarodowym aktem ochrony danych osobowych”[352]. Warto podkreślić, że do połowy lat siedemdziesiątych XX w. Komitet Ministrów Rady Europy przyjmował rezolucje w sprawie ochrony danych osobowych, powołując się na art. 8 *Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności*[353].

Konwencja nr 108 ma zastosowanie do wszelkich operacji przetwarzania danych odbywających się w sektorze zarówno prywatnym, jak i publicznym, w tym również do przetwarzania danych przez organy sądowe czy w ramach egzekwowania prawa. Jej dość ogólne postanowienia okazały się jednak niewystarczające. Pojawiła się potrzeba, aby dostosować generalne zasady do specyficznych wymogów sektorowych. Dzięki tzw. sektorowemu ujęciu ochrony danych osobowych, Komitet Ministrów Rady Europy przyjął wiele zaleceń i rekomendacji dla rządów państw członkowskich[354].

Celem konwencji nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z 28 stycznia 1981 r. jest zapewnienie osobom fizycznym ochrony ich danych osobowych przed nadużyciami, które mogą towarzyszyć gromadzeniu i przetwarzaniu danych, jak również uregulowanie transgranicznego przepływu danych osobowych[355].

Zgodnie z art. 1 konwencji każda osoba fizyczna, bez względu na narodowość lub miejsce zamieszkania, ma mieć zagwarantowane

„poszanowanie jej praw i podstawowych wolności na terytorium każdej ze stron konwencji, a w szczególności jej prawa do prywatności w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych". W preambule konwencji nr 108 zostało podkreślone, że motywem przewodnim tego międzynarodowego aktu jest wypracowanie kompromisu między ochroną praw i podstawowych wolności, w tym prawa do prywatności, a wolnością przepływu informacji bez względu na granice. Kompromis ten został określony jako „szczególny problem ścierania się prawa do informacji z prawem do ochrony danych osobowych". Niemniej jednak głównym celem konwencji jest „wprowadzenie ujednoliconej ochrony danych osobowych w krajach europejskich i zharmonizowanie jej z ideą swobodnego przepływu danych w obrębie państw członkowskich"[356].

Zasady gromadzenia i przetwarzania danych osobowych, ustanowione w konwencji nr 108, dotyczą w szczególności rzetelnego i zgodnego z prawem gromadzenia oraz automatycznego przetwarzania danych, które powinny być gromadzone dla określonych i usprawiedliwionych celów, oraz nie mogą być wykorzystywane w sposób niezgodny z tymi celami czy przechowywane przez okres dłuższy, niż jest to wymagane. Dane te muszą być również odpowiednie, rzeczowe, niewykraczające poza potrzeby wynikające z celów, a także dokładne i w razie potrzeby uaktualniane. Dodatkowo konwencja nr 108 wprowadza zakaz, przy braku odpowiednich gwarancji prawnych ochrony, przetwarzania danych szczególnie chronionych (*sensitive data)*, tj. dotyczących m.in. rasy, poglądów politycznych, stanu zdrowia, przekonań religijnych, życia seksualnego czy karalności danej osoby. Niestety nie precyzuje, na czym miałyby polegać te gwarancje ochrony (wdrożone przez prawo wewnętrzne strony konwencji).

Konwencja nr 108 przyznaje uprawnienia podmiotom danych, „w tym prawo do ustalenia, czy istnieje w ogóle zautomatyzowany zbiór danych osobowych zawierający dane dotyczące osoby i w konsekwencji – prawo do poznania podstawowych celów utworzenia zbioru, tożsamości, miejsca zamieszkania lub siedziby

administratora zbioru”[357]. Ograniczenia praw podmiotów danych wynikające z art. 9 ust. 2 konwencji nr 108 jest dopuszczalne jedynie, gdy zagrożone są nadrzędne interesy, takie jak ochrona i interesy finansowe państwa, utrzymanie porządku i bezpieczeństwa publicznego, zwalczanie przestępczości, ochrona osoby, której dane dotyczą, bądź ochrona praw lub wolności innych osób. Konwencja przewiduje swobodny przepływ danych osobowych między sygnatariuszami, niemniej jednak może on zostać ograniczony w przypadku, gdy regulacje prawne danego państwa (strony konwencji) nie zapewniają równoważnego stopnia ochrony[358].

Konwencja nr 108 została zmieniona w 1999 r.[359], aby umożliwić państwom Unii Europejskiej przystąpienie do niej. Następnie w 2001 r. został przyjęty protokół dodatkowy do tej konwencji[360], który wprowadził przepisy dotyczące transgranicznego przepływu danych do państw trzecich niebędących stronami konwencji oraz obowiązek ustanowienia krajowych organów nadzorujących ochronę danych.

4.1.2. INTERPOL W WALCE Z CYBERTERRORYZMEM

Interpol jest Międzynarodową Organizacją Policji Kryminalnej, której początki sięgają 1914 r. W 1923 r. na II Kongresie ustanowiono Międzynarodowy Komisariat Policji Kryminalnej, a w 1946 r. utworzono główną siedzibę tej organizacji w Paryżu. Polska jest jej aktywnym członkiem.

Aktualnie członkami Interpolu są 194 państwa[361]. Działalność Interpolu w zwalczaniu terroryzmu zaczęła się w 1986 r., kiedy na 55. Sesji Zgromadzenia Ogólnego organizacji utworzono Grupę TE (ds. terroryzmu), która skupiła się na:

- współpracy z organizacjami międzynarodowymi w zakresie zapobiegania terroryzmowi i zwalczania go,
- organizowaniu szkoleń dla funkcjonariuszy policji z różnych krajów zajmujących się zwalczaniem terroryzmu,
- gromadzeniu i udostępnianiu informacji o ugrupowaniach terrorystycznych, a także opracowywaniu materiałów informacyjnych dotyczących terroryzmu[362].

Głównym celem działalności Interpolu jest wspieranie organów policji kryminalnych na świecie, wymiana informacji oraz oferowanie wsparcia i narzędzi do efektywnego ścigania przestępstw. Kluczowe miejsce w działalności organizacji zajmuje utworzony w 2002 r. globalny system łączności I-24/7, dzięki któremu krajowe biura Interpolu mogą zdalnie uzyskać dostęp do baz danych, dzielić się pilnymi informacjami ze wszystkimi członkami Interpolu 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.

Interpol jest szczególnie zaangażowany w globalną walkę z cyberprzestępczością. Większość przestępstw popełnianych w cyberprzestrzeni ma charakter ponadnarodowy i transgraniczny, Interpol jest więc naturalnym partnerem dla krajowych organów ścigania. Jerzy Kosiński[363] wskazuje, że „rola Interpolu w zwalczaniu cyberprzestępczości opiera się na prowadzeniu szkoleń, działaniach operacyjnych i działaniach mających zapewniać nadążanie służbom policyjnym za nowymi zagrożeniami. Realizowana jest przez:

- wspieranie wymiany informacji między państwami członkowskimi za pośrednictwem regionalnych grup roboczych i konferencji;
- prowadzenie szkoleń w celu budowania i utrzymywania standardów zawodowych;
- koordynowanie i wspieranie operacyjnych działań międzynarodowych;
- ustanowienie globalnej listy oficerów kontaktowych ds. zwalczania cyberprzestępczości dostępnych przez całą dobę siedem dni w tygodniu;
- pomaganie krajom członkowskim w przypadku wystąpienia aktów cyberprzestępców lub ścigania sprawców cyberprzestępczości przez dostarczanie usług i dostęp do bazy danych;
- rozwijanie strategicznego partnerstwa z innymi organizacjami międzynarodowymi i podmiotami sektora prywatnego;
- identyfikację pojawiających się zagrożeń i udostępnianie tej wiedzy państwom członkowskim;

- zapewnienie dostępu do bezpiecznego portalu internetowego z informacjami operacyjnymi i dokumentami”[364].

W roku 2014 w Singapurze uruchomiono Globalny Zespół Innowacji Interpolu (IGCI)[365]. To instytucja badawcza, która ma na celu rozwój metod identyfikacji przestępstw i przestępców, prowadzenie innowacyjnych szkoleń, wsparcie operacyjne i współpracę między członkami. Celem ośrodka jest zapewnienie jednostkom policji na całym świecie narzędzi i zdolności do konfrontacji z coraz bardziej pomysłowymi i skomplikowanymi metodami działania cyberprzestępców. W 2018 r. Organizacja Narodów Zjednoczonych określiła Interpol jako największą i najstarszą międzynarodową organizację policyjną na świecie oraz jako wyjątkowego partnera we wdrażaniu licznych celów zrównoważonego rozwoju do 2030 r. (SDGs)[366].

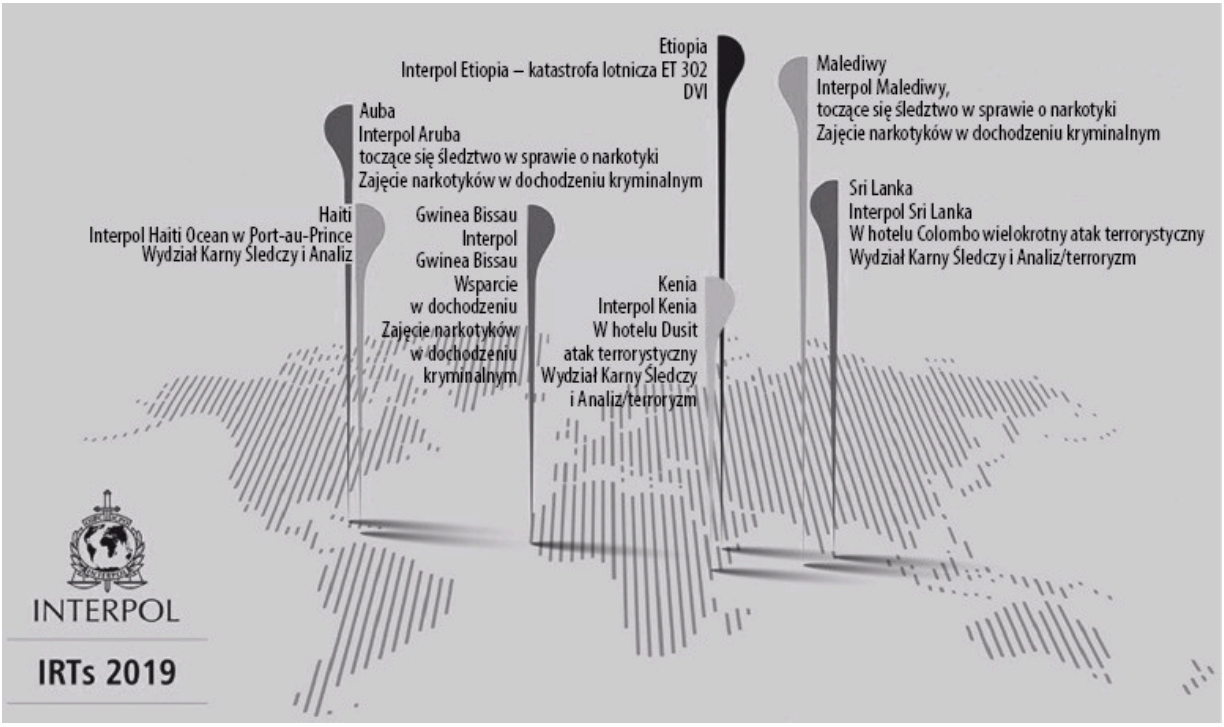
Do głównych celów działalności IGCI należy budowanie potencjału i przeprowadzanie szkoleń, wsparcie operacyjne i śledcze oraz bezpieczeństwo cyfrowe. Cel czwarty realizowany jest przez:

- zwiększanie cyberbezpieczeństwa i przeciwdziałanie cyberprzestępczości;
- funkcjonowanie laboratorium kryminalistycznego wspierającego postępowania w sprawach o cyberprzestępstwa;
- badanie protokołów, narzędzi, usług oraz analizy trendów aktów cyberprzestępców;
- ochronę społeczności przez tworzenie standardów, edukację publiczną i zarządzanie bezpieczeństwem Internetu;
- ochronę infrastruktury krytycznej[367].

Interpol podejmuje działania nie tylko ściśle związane z terroryzmem i cyberprzestępczością. Równie istotne są prace dotyczące oszustw, które coraz częściej są popełniane za pomocą cyberprzestrzeni. Do oszustw finansowych popełnionych za pomocą ICT Interpol zalicza: pranie brudnych pieniędzy, oszustwa związane z kartami płatniczymi, walutami i sfałszowanymi dokumentami oraz oszustwa związane z inżynierią społeczną (*phishing*).

W ramach Interpolu powołane są również komórki zajmujące się przestępstwami przeciwko dzieciom. Przestępcy nie tylko wymieniają się materiałami zawierającymi pornografię dziecięcą, ale także wykorzystują Internet do nawiązania kontaktu z nieletnimi za pośrednictwem czatów i sieci społecznościowych[368].

Jako jedno z głównych cyberzagrożeń Interpol wymienia tzw. Darknet, czyli ciemną sieć[369], która jest częścią cyberprzestrzeni ukrytą przed normalnymi użytkownikami. Nazywana jest również „Deep Web", czyli głęboką siecią. Darknet jest siecią wykorzystywaną przez przestępców, którzy poruszają się w niej za pomocą specjalistycznego oprogramowania, ukrywającego ich prawdziwą tożsamość. Darknet jest wykorzystywany do nielegalnych transakcji takich, jak sprzedaż narkotyków i broni, nielegalny hazard, handel podrobionymi dokumentami tożsamości czy pornografia dziecięca. Skomplikowane narzędzia szyfrowania i programy mające na celu ukrycie tożsamości posługujących się nimi osób używane do komunikowania się w Darknecie stawiają przed organami ścigania wiele wyzwań dotyczących identyfikacji i lokalizacji przestępców.



RYSUNEK 4.2
Zespoły reagowania na incydenty przez Interpol

Źródło: https://www.interpol.int/en/How-we-work/INTERPOL-response-teams (dostęp: 30.07.2020).

4.1.3. ORGANIZACJA NARODÓW ZJEDNOCZONYCH W WALCE Z CYBERTERRORYZMEM

Jednym z pierwszych dokumentów ONZ, które odnosiły się do czynów dokonywanych za pośrednictwem przestrzeni wirtualnej, czyli przestępstw komputerowych, były rezolucja Zgromadzenia Ogólnego ONZ nr 45/1213 oraz rezolucja nr 45/12164[370] dotycząca przestępstw związanych z wykorzystaniem komputerów[371].

Pierwsza została przyjęta 14 grudnia 1990 r. w wyniku obrad VIII Kongresu Narodów Zjednoczonych, który się odbywał od 28 sierpnia do 7 września 1990 r. w Hawanie, a jego tematem było zapobieganie przestępczości i postępowanie z przestępcami. Rezolucja ta wzywa państwa członkowskie do intensyfikacji wysiłków skierowanych na skuteczne zwalczanie nadużyć komputerowych, w szczególności przez:

- wprowadzenie odpowiednich zmian do ustawodawstwa karnego materialnego i procesowego w celu dostosowania istniejących definicji przestępstw oraz przepisów dotyczących środków przymusu i dopuszczalności dowodów do ścigania nadużyć komputerowych oraz pozbawienia ich sprawców nielegalnie uzyskanych korzyści;
- usprawnienie zabezpieczeń systemów komputerowych, uwzględniając przy tym problemy związane z ochroną prywatności oraz praw i wolności obywatelskich;
- podjęcie kroków mających na celu uwrażliwienie opinii publicznej oraz organów ścigania i wymiaru sprawiedliwości na znaczenie problemu zapobiegania przestępczości komputerowej.

Druga rezolucja podkreślała konieczność wprowadzenia przestępstw komputerowych do porządków legislacyjnych państw i

była podstawą do wydania w 1994 r. poradnika *International review of criminal policy – United Nations Manual on the prevention and control of computer – related crime*, dotyczącego zapobiegania cyberprzestępczości i kontroli cyberprzestępstw[372]. Od 1998 r. cyberbezpieczeństwo stało się stałym punktem obrad Walnego Zgromadzenia ONZ, a także tematem kilkunastu rezolucji wydanych nie tylko przez Walne Zgromadzenie, ale także organizacje działające w ramach ONZ, w szczególności Międzynarodowy Związek Telekomunikacyjny (International Telecommunication Union – ITU)[373].

Akty prawne i dokumenty przyjęte na forum Organizacji Narodów Zjednoczonych odnoszą się do przestępczości popełnianej w cyberprzestrzeni. Są to:

- Konwencja wiedeńska z 11 kwietnia 1980 r.[374] dotycząca sprzedaży towarów – celem zapisanym w art. 2 było wprowadzenie nowoczesnego, jednolitego i sprawiedliwego systemu międzynarodowej sprzedaży towarów i tym samym wprowadzenie pewności wymiany handlowej oraz zmniejszenie kosztów transakcyjnych. Ma ona zastosowanie do sprzedaży towarów między stronami mającymi siedziby handlowe w różnych państwach (art. 3). Art. 4 wyłącza jej stosowanie w odniesieniu do sprzedaży towarów zakupionych do użytku osobistego, rodzinnego lub do użytku w gospodarstwie domowym oraz w stosunku do sprzedaży w drodze licytacji, egzekucji, sprzedaży energii elektrycznej, okrętów, statków oraz udziałów, akcji, papierów wartościowych, tytułów inwestycyjnych i pieniędzy. Konwencji nie stosuje się również do umów o świadczenie usług.
- Konwencja ONZ przeciwko międzynarodowej przestępczości zorganizowanej (UNTOC) przyjęta przez Zgromadzenie Ogólne ONZ 15 listopada 2000 r.[375] reguluje międzynarodowe standardy walki z międzynarodowymi zorganizowanymi grupami przestępczymi oraz korupcją i praniem brudnych pieniędzy. Konwencja nakłada na strony obowiązek wprowadzenia odpowiedniego reżimu prawnego dla banków i innych instytucji

finansowych, które mogą być podatne na pranie pieniędzy w taki sposób, by podmioty te wprowadziły odpowiednie procedury identyfikacji klienta, prowadzenia dokumentacji oraz informowania o podejrzanych transakcjach. Państwa strony tej konwencji zobowiązały się również do poszerzenia współpracy międzynarodowej, wymiany informacji oraz przeprowadzania szkoleń dla organów ścigania w zakresie inwigilacji elektronicznej, metod wykorzystywanych do zwalczania międzynarodowej przestępczości zorganizowanej popełnianej przy wykorzystaniu komputerów, sieci telekomunikacyjnych lub innych form nowoczesnych technologii.

- Rezolucja Zgromadzenia Ogólnego ONZ nr 53/70 z 3 grudnia 1998 r.[376] dotycząca przestępczości cybernetycznej, cyberterroryzmu i wojen cybernetycznych *Rozwój w dziedzinie informacji i telekomunikacji w kontekście międzynarodowego bezpieczeństwa* wzywa państwa do informowania Sekretariatu Generalnego o rezultatach i ocenach obserwacji w następujących zakresach: bezpieczeństwa informacji, określenia standardów bezpieczeństwa i opracowania zasad na poziomie międzynarodowym, mających na celu wzmocnienie światowego systemu informacji, telekomunikacji i zwalczania przestępczości oraz terroryzmu.
- Rezolucja ONZ nr 2011/33[377] w sprawie skutecznego zapobiegania i ścigania przestępstw związanych z seksualnym wykorzystaniem małoletnich dotyczy problemu dziecięcej pornografii, również w kontekście przepisów i instrumentów zawartych w konwencji o cyberprzestępczości. Rezolucja zachęca państwa członkowskie do podjęcia odpowiednich kroków prawnych w prawodawstwie krajowym w celu zapobiegania wykorzystaniu mass mediów, technologii informacyjnych, w tym Internetu, do seksualnego wykorzystania małoletnich. Jest nawiązaniem do wcześniejszych rezolucji Zgromadzenia Ogólnego nr 55/63 z 4 grudnia 2000 r., nr 56/121 z 19 grudnia 2001 r. i 64/211 z 21 grudnia 2009 r. w sprawie zwalczania przestępczego nadużycia technologii

informacyjnych. Potwierdza również założenia przyjęte w rezolucji nr 2004/26 z dnia 21 lipca 2004 r. zatytułowanej *Współpraca międzynarodowa w zakresie zapobiegania, dochodzenia, ścigania i karania oszustwa, nadużycia karnego i fałszowania tożsamości i powiązanych przestępstw* oraz rezolucji nr 2007/20 z 26 lipca 2007 r. zatytułowanej *Współpraca międzynarodowa w sprawie zapobiegania, dochodzenia, ścigania i karania oszustw gospodarczych i przestępstw związanych z tożsamością*, a także rezolucji w sprawie wymiaru sprawiedliwości w sprawach karnych nr 16/2 z 27 kwietnia 2007 r. *Skuteczne zapobieganie przestępczości i postępowanie w sprawach karnych w zwalczaniu wykorzystywania seksualnego dzieci*.

4.2
PRAWO UNIJNE WOBEC CYBERTERRORYZMU

4.2.1. PRAWO PIERWOTNE UNII EUROPEJSKIEJ WOBEC CYBERTERRORYZMU

W prawie Unii Europejskiej przeciwdziałanie cyberterroryzmowi przez długi czas nie miało właściwego miejsca. Za początki współdziałania państw członkowskich UE w zakresie przeciwdziałania cyberterroryzmowi i zwalczania go należy uznać lata dziewięćdziesiąte XX w., kiedy odnotowano znaczne wzmożenie aktywności ataków w Internecie.

Dopiero wraz z wprowadzeniem tyt. VI TUE przez Traktat z Maastricht po raz pierwszy działania UE zostały wyposażone w podstawę prawną, dzięki której wzmocniono je i rozszerzono przez Traktat z Amsterdamu. Najważniejszym przepisem był art. 2 TUE, który przewidywał utrzymanie i rozwój Unii jako przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Bezpieczeństwo wewnętrzne leży u podstaw tego celu i jest jasne, że główny nacisk,

jaki został położony w art. 29 TUE, ma polegać na zapewnieniu „obywatelom wysokiego poziomu bezpieczeństwa". Cel ten został powtórzony w sposób niemal identyczny w art. 61e TWE, co oznacza, że Unii jednoznacznie udzielono mandatu jako dostawcy bezpieczeństwa wewnętrznego, co samo w sobie jest jedną z najważniejszych innowacji. Artykuł 29 ust. 2 wymieniał terroryzm jako formę przestępczości, przeciwko której w szczególności powinny być skierowane odpowiednie działania[378].

W 1997 r. Rada przyjęła całościowy plan zwalczania przestępczości zorganizowanej[379], zaproponowany przez Grupę Wysokiego Szczebla utworzoną na mocy decyzji Rady UE z grudnia 1996 r. Plan zawierał wezwanie do uznania za przestępstwo przez państwa członkowskie udziału w organizacji przestępczej oraz definicję tego pojęcia. Wzywał ponadto do jak najszybszego zawarcia konwencji o wzajemnej współpracy w sprawach karnych i ujednolicenia przepisów prawa państw członkowskich w tej dziedzinie. Uznał również, że współpraca policyjna musi być wspierana przez współpracę sądową. Uzupełnienie planu stanowi rezolucja Rady z 12 grudnia 1998 r.[380], która zakłada, że należy na wszelki możliwy sposób zwalczać przestępczość zorganizowaną. Dlatego Unia wyznaczyła siedem celów strategicznych w zakresie polityki antyterrorystycznej:

- pogłębianie międzynarodowego konsensusu i wzrost wysiłków społeczności międzynarodowej związanej z walką z terroryzmem;
- ograniczenie dostępu terrorystów do środków finansowych i gospodarczych;
- rozwój instrumentów instytucji UE i państw członkowskich w celu zidentyfikowania terrorystów, ścigania ataków terrorystycznych i zapobiegania im;
- zapewnienie bezpieczeństwa transportu międzynarodowego i skuteczności systemu kontroli granicznej;
- rozwijanie umiejętności Unii Europejskiej i państw członkowskich w zakresie radzenia sobie z konsekwencjami ataku terrorystycznego;

- znajdowanie czynników, które przyczyniają się do terroryzmu;
- działania docelowe w stosunkach zewnętrznych Unii z państwami trzecimi, których zdolność do walki z terroryzmem musi być wzmocniona.

4.2.1.1. Traktat z Maastricht

Traktat o Unii Europejskiej z 1992 r., który wszedł w życie z dniem 1 listopada 1993 r., utworzył III filar, uregulował kwestie współpracy w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych w art. K.1–K.9. Z uwagi na brak stosownych regulacji traktatowych wcześniejsza współpraca odbywała się jednak poza wspólnotami[381]. W tym celu wykorzystywano np. grupę TREVI. Podstawę działania stanowiły klasyczne formy prawa międzynarodowego, m.in. umowy międzynarodowe, rezolucje, zalecenia i wnioski. W traktacie po raz pierwszy zapisano zadania zapobiegania i zwalczania przestępczości oraz współpracy międzyrządowej w tym zakresie. Na mocy TUE walka z terroryzmem międzynarodowym stała się jedną z dziedzin objętych współpracą w prawie pierwotnym Unii w zakresie wymiaru sprawiedliwości i spraw wewnętrznych, co oznaczało zastąpienie przez III filar dotychczasowych form współpracy i w tak wyraźny sposób potraktowanie problemu terroryzmu. Powołano również Europol[382].

W preambule do TUE państwa członkowskie zgodziły się dążyć do umożliwienia swobodnego przepływu osób przy jednoczesnym zapewnieniu „bezpieczeństwa swoich narodów przez włączenie do niniejszego traktatu postanowień dotyczących wymiaru sprawiedliwości i spraw wewnętrznych”[383]. Zgodnie z postanowieniami Traktat z Maastricht, w dawnym art. K.1, dość szeroko zakreślił następujące obszary, które zostały zaliczone do realizacji celów Unii w ramach III filaru:

- współpracę sądową w sprawach cywilnych,
- współpracę sądową w sprawach karnych,
- współpracę celną,

- współpracę policyjną w celach zapobiegania i walki z terroryzmem, nielegalnym handlem narkotykami i innymi poważnymi formami międzynarodowej przestępczości,
- politykę azylową i migracyjną,
- zwalczanie narkotyków i nadużyć finansowych.

Dawny art. K.1. (późniejszy art. 29 TUE) sformułował cele i instrumenty współpracy w ramach III filaru. Celem podstawowym Unii, nienaruszającym kompetencji Wspólnoty, jest zapewnienie jej obywatelom wysokiego poziomu bezpieczeństwa w dziedzinie wolności, bezpieczeństwa i sprawiedliwości. W tym zakresie artykuł ten powtarzał zapis z art. 2 ust. 4 traktatu, a tym samym nie stanowił indywidualnego celu tylko dla III filaru. Wiązał się bezpośrednio ze swobodą przepływu osób i osiedlania się, polityką wizową, azylową i imigracyjną, zasadą antydyskryminacyjną, polityką ochrony zdrowia przed narkotykami czy nadużyciami finansowymi. Ten cel miał być osiągany za pomocą celów pośrednich przez zapobieganie i zwalczanie przestępczości, ściślejszej współpracy policji, organów sądowych i władz celnych[384], a także przez zbliżanie ustawodawstwa karnego.

Traktat z Maastricht enumeratywnie wyliczał przestępstwa, tj. terroryzm czy handel narkotykami, stanowiące przedmiot współpracy karnej, natomiast Traktat z Amsterdamu poszerzył tę listę o kolejne przestępstwa i zmienił jej charakter z zamkniętej na przykładową, o czym świadczy sformułowanie „w szczególności".

Na mocy Traktatu z Maastricht do wspólnego zainteresowania w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych zaliczono m.in. współpracę policyjną w celu zapobiegania terroryzmowi i walki z nim, a także organizację systemu wymiany informacji w ramach Europolu (art. K.1 pkt 9 tyt. VI TUE). W wyniku włączenia do III filaru Unii Europejskiej współpracy w zakresie zapobiegania i walki z terroryzmem[385] zlikwidowano I Grupę Roboczą TREVI, a kompetencje w tym zakresie uzyskała Grupa Robocza ds. Terroryzmu działająca w ramach Grupy Kierowniczej II, podległej Komitetowi Koordynacyjnemu (Komitet K.4).

Zgodnie z art. K.2–K.3 Traktatu z Maastricht zasadniczym, choć nie jedynym rodzajem wspólnych działań miała być współpraca policyjna realizowana za pośrednictwem Europolu, jednak jej budowa przebiegała z dużymi trudnościami. Pojęcie „współpracy policyjnej" było tu rozumiane szeroko i dotyczyło każdego rodzaju współpracy związanej ze zwalczaniem i przeciwdziałaniem przestępczości. Przez długie lata współpraca sądowa pozostawała raczej w sferze dyskusji niż działań. Dominującą formą współdziałania w III filarze pod względem aktywności była współpraca policyjna, natomiast na podstawie regulacji zawartych we wspomnianym traktacie rozwijała się współpraca polityczna i operacyjna państw członkowskich UE w ramach Rady UE.

Problematykę form współpracy regulował art. K.3 TUE, który przewidywał wzajemne informowanie się i koordynowanie swoich działań[386] przez państwa członkowskie w ramach Rady. Upoważniał Radę do wydawania wspólnych stanowisk i opracowywania konwencji przedkładanych następnie państwom członkowskim do przyjęcia (d. art. K.5). Problematyka ta nie była jedynie ograniczona do obszaru współpracy policyjnej i sądowej w sprawach karnych. W jej skład wchodziły także te dziedziny, które na podstawie TA zostały przeniesione do I filaru.

Dawny art. K.3 ust. 2c TUE nie regulował kompetencji ETS w zakresie III filaru. Przewidywał jedynie, że poszczególne konwencje zawierane w ramach ówczesnego III filaru mogły przyznać Trybunałowi jurysdykcję w zakresie interpretacji lub rozwiązywania sporów dotyczących ich stosowania. Mimo że kompetencje Trybunału w tym zakresie są znacznie zawężone, należy stwierdzić, że na podstawie TA przyznano mu dość istotne uprawnienia w obszarze współpracy policyjnej i sądowej[387].

Przewodniczący i Komisja natomiast zgodnie z d. art. K.6. ust. 1 mieli jedynie obowiązek regularnie informować Parlament Europejski o pracach prowadzonych w niniejszych dziedzinach. Parlament Europejski mógł, stosownie do art. K.6 ust. 3, kierować do Rady pytania lub formułować pod jej adresem zalecenia, a co roku

przeprowadzał debatę w sprawie postępów w realizacji dziedzin objętych niniejszym tytułem.

Na podstawie art. K.4 powołano Komitet Koordynacyjny, w którego skład wchodzą wyżsi urzędnicy. Oprócz sprawowania funkcji koordynacyjnej Komitet wydaje opinie dla Rady, na jej wniosek lub z własnej inicjatywy, przyczynia się, bez uszczerbku dla Traktatu ustanawiającego Wspólnotę Europejską, do przygotowywania prac Rady w dziedzinach, o których mowa w art. K.1 i zgodnie z warunkami określonymi w Traktacie ustanawiającym Wspólnotę Europejską.

Istotne znaczenie miał art. K.9, ponieważ umożliwiał Radzie, działającej na wniosek Komisji lub państwa członkowskiego, podjęcie decyzji o uwspólnotowieniu spraw stanowiących przedmiot wspólnego zainteresowania (z wyjątkiem współpracy sądowej w sprawach karnych, współpracy celnej i policyjnej). Przeszkodą jego praktycznego zastosowania był jednak wymóg jednomyślności państw członkowskich oraz konieczność ratyfikacji decyzji zgodnie z prawem wewnętrznym państw. Z tego powodu stał się martwym przepisem[388].

Za podstawową formę współpracy w ramach TUE uznano istniejącą już wcześniej współpracę międzyrządową. Stało się to podstawą do podejmowania uchwał, zaleceń i wniosków w sytuacjach, gdy państwa z różnych względów nie chciały przyjąć innego dokumentu. Typowymi instrumentami wykorzystywanymi w III filarze do tworzenia norm bezpośrednio wiążących były konwencje. Istotne jest również, że do 2001 r. nie opracowano w UE żadnego projektu międzynarodowego bezpośrednio dotyczącego zwalczenia terroryzmu, przyjęto natomiast konwencje poruszające pośrednio tę problematykę. Z kolei wspólne działania i wspólne stanowiska nie zostały jasno określone i były uznawane, co do zasady, za przedsięwzięcia niewiążące prawnie. W praktyce tyt. VI TUE niewiele zmienił w dotychczasowej współpracy państw członkowskich w ramach spraw wewnętrznych i wymiaru sprawiedliwości[389].

4.2.1.2. Traktat z Amsterdamu

Traktat z Amsterdamu został podpisany 2 października 1997 r. i wszedł w życie 1 maja 1999 r. Dokonał ogromnych zmian w zakresie III filaru[390], ponieważ odważniej i bardziej zdecydowanie przeprowadził jego reformę. Został określony jako „Współpraca policyjna i sądowa w sprawach karnych", tym samym polityka wizowa, azylowa i migracyjna oraz współpraca cywilna zostały przeniesione do I filaru.

Zgodnie z treścią art. 29 TUE: „Celem Unii jest zapewnienie obywatelom wysokiego poziomu bezpieczeństwa w dziedzinie wolności, bezpieczeństwa i sprawiedliwości przez opracowywanie wspólnych działań państw członkowskich w dziedzinie współpracy policyjnej i sądowej w sprawach karnych oraz przez zapobieganie i zwalczanie przestępstw zorganizowanych i innych, a w szczególności terroryzmu"[391]. Traktat z Amsterdamu dokładniej określił cele współpracy, a jedną z jej płaszczyzn stało się zbliżanie zasad prawa karnego, w szczególności zharmonizowania znamion przestępstw oraz ustalenie dolnej granicy wymiaru kary m.in. w odniesieniu do terroryzmu[392].

Istotną zmianą, jaka zaszła w wyniku podpisania tego traktatu, było wprowadzenie nowych instrumentów prawnych w zakresie III filaru – decyzji ramowych i decyzji w sprawach pozostałych. Traktat dokonał też daleko idących zmian w zakresie porządku prawnego Schengen. Na mocy protokołu włączającego dorobek Schengen w ramy Unii Europejskiej przepisy *Konwencji Wykonawczej do Układu z Schengen* zostały inkorporowane zarówno do I filaru UE w zakresie zniesienia kontroli na wewnętrznych granicach oraz przepływu osób, jak i III filaru – w odniesieniu do współpracy policji i Systemu Informacji Schengen (art. 39–91 tyt. III i art. 92–119 tyt. IV).

W Traktacie z Amsterdamu dokładniej określono cele współpracy, a jedną z płaszczyzn współpracy stało się zbliżanie zasad prawa karnego, w szczególności zharmonizowania znamion przestępstw oraz ustalenie dolnej granicy wymiaru kary, w odniesieniu m.in. do terroryzmu[393].

Tak określonym celom współpracy w III filarze UE mają służyć następujące instrumenty:

- ścisła współpraca sądowa w sprawach karnych,
- zbliżanie w koniecznym zakresie przepisów karnych państw członkowskich,
- ścisła współpraca policyjna obejmująca nie tylko państwową współpracę policyjną i celną, ale także współpracę za pośrednictwem Europolu.

Uszczegółowienie i kontynuacja postanowień z art. 29 TUE znalazły się w art. 30 i art. 31 traktatu. Dokonując całkowitej przebudowy III filaru Unii Europejskiej, Traktat z Amsterdamu stworzył te zapisy praktycznie od nowa, reformując w ten sposób współpracę policyjną. Tym samym w traktacie znalazła się regulacja bardziej obszerna, zwarta i tworząca dalej idące obowiązki dla państw i instytucji Unii. Artykuł 30 TUE w brzmieniu ustalonym przez TA przewiduje wspólne działanie w zakresie współpracy policyjnej. Ten typ współdziałania był już wprawdzie wymieniony w III filarze Traktatu z Maastricht, ale nie tak obszernie. Traktat z Amsterdamu uznał kompetencje operacyjne Europolu: gromadzenie, przechowywanie, przetwarzanie, analizowanie i wymianę istotnych informacji (art. 30 ust. 1 lit. b i art. 30 ust. 2), wymienił również przykładowo różne formy współpracy policyjnej między odpowiednimi organami (art. 30 ust. 1 lit. a, c i d)[394]. Przyjęta forma współpracy jest daleka od ujednolicania systemów prawa karnego. Mamy tu do czynienia z minimalną harmonizacją polityki kryminalnej państw członkowskich, prowadzącą do postrzegania w ten sposób pewnych zachowań przestępczych. Formuła ta jest niezwykle ostrożna ze względów konstytucyjnych i ma na celu zachowanie niezależności systemów państw członkowskich. Jest to raczej tendencja zmierzająca w stronę standardów minimalnych, poniżej których nie można już zejść[395].

W art. 34 TUE uregulowano na nowo problematykę d. art. K.3. TUE, zawężając formy działania jedynie do obszaru współpracy policyjnej i sądowej w sprawach karnych. Znajduje on zastosowanie do znacznie węższej sfery niż początkowy obszar Unii

Europejskiej[396]. Zgodnie z art. 34 ust. 2 istnieją cztery główne instrumenty, wspólne stanowiska, które mają służyć określeniu pozycji w konkretnej sprawie, które członkowie Unii zgodnie z art. 37 TEU mają obowiązek bronić na arenie międzynarodowej. Niektórzy twierdzą, że pod tym pojęciem należy rozumieć wytyczanie działań na płaszczyźnie samej Unii[397]. Decyzje ramowe z jednej strony są uderzająco podobne do dyrektyw, z drugiej – do postanowień programowych. Obie formy instrumentów są wiążące co do celu, który ma być za ich pomocą implementowany, przez co mają służyć zbliżaniu porządków prawnych państw członkowskich. Pozostawiają w ten sposób swobodną decyzję w doborze środków służących do osiągnięcia danego rezultatu, czyli technikę ich implementacji. Różnica polega na tym, że decyzje ramowe nigdy nie mogą wywołać skutku bezpośredniego, gdy dyrektywy w określonych okolicznościach taki skutek mogą osiągnąć. Z kolei „zwykłe" decyzje różnią się od decyzji ramowych tym, że podejmowane są przez Radę UE większością kwalifikowaną w innych celach niż harmonizacja przepisów w ramach III filaru. Kategorią stanowiącą uzupełnienie decyzji z III filaru są środki wykonawcze. Ostatnim instrumentem są wiążące akty prawa międzynarodowego, które w zależności od tego, kto jest ich stroną, traktat nazywa konwencją albo umową międzynarodową z państwem trzecim. Faza wstępna spoczywa na Radzie, która opracowuje tekst konwencji, a następnie zaleca jego przyjęcie państwom członkowskim. Na mocy regulacji TA Rada powinna konsultować wszelkie decyzje z Parlamentem Europejskim na trzy miesiące przed ich podjęciem. Pośrednio ważne miejsce przyznano również parlamentom państwowym[398].

Zgodnie z treścią art. 35 kompetencje ETS są wyraźnie wyłączone w stosunku do wykonywania funkcji policyjnych. W żadnym razie Trybunał nie może zajmować się badaniem legalności lub proporcjonalności czynności operacyjnych policji i innych organów podejmowanych przez państwa członkowskie w celu zapewnienia porządku publicznego i bezpieczeństwa wewnętrznego[399]. Trybunał natomiast może wydawać orzeczenia prejudycjalne w kwestiach dotyczących interpretacji oraz mocy prawnej aktów prawa wtórnego

III filaru. Może także kontrolować legalność aktów prawnych i rozstrzygać spory między państwami oraz państwami a Komisją. O ile procedura kontroli jest podobna do tej przewidzianej w I filarze, to inne są krąg podmiotów uprawnionych (węższy) i przedmiot badania legalności aktów[400].

Traktat z Amsterdamu w miarę kompleksowo reguluje w art. 39 rolę Parlamentu Europejskiego w III filarze. W TUE Parlament nie posiadał żadnych uprawnień decyzyjnych, a jedynie doradcze i konsultacyjne (d. K.6. akp. 1 i 3). TA dokonał daleko idących konkretyzacji. Teraz przy uchwalaniu wszelkich instrumentów w ramach III filaru, z wyjątkiem wspólnych stanowisk, wymaga się od Rady uprzedniego uzyskania opinii Parlamentu. Chociaż wynik konsultacji nie jest wiążący dla Rady, powinien być ze swej istoty brany pod uwagę. Parlament posiada również istotny instrument wpływania na budżet III filaru przez dokonywanie zmian i modyfikacji projektu budżetowego. W ten sposób może również wpływać na kierunki rozwoju współpracy policyjnej i sądowej w sprawach karnych.

Mimo że wszystkie te kompetencje do działania miały charakter niewyłączny i pozostawały w sferze międzyrządowej współpracy (tyt. VI TUE), dały znaczne możliwości szerszej współpracy między państwowymi organami policji i wymiaru sprawiedliwości, wzmocnienia roli Europolu i harmonizacji państwowych przepisów prawa karnego. Dwa z uwspólnotowionych obszarów tyt. IV TWE miały natomiast znaczenie dla terroryzmu. Były to:

- normy i procedury, których powinny przestrzegać państwa członkowskie przy wykonywaniu kontroli osób na granicach zewnętrznych (art. 62.2a TWE);
- reguły dotyczące wiz na pobyt nie dłuższy niż trzy miesiące, w tym wykaz państw trzecich, których obywatele muszą posiadać wizy podczas przekraczania granic zewnętrznych (art. 62.2b TWE)[401].

Instrumenty prawne zależały od podstawy prawnej. W uwspólnotowionych obszarach tyt. IV TWE dobrze ustalonymi instrumentami WE były głównie rozporządzenia i dyrektywy.

Pierwotnymi instrumentami w międzyrządowej domenie tyt. VI TUE były decyzje i decyzje ramowe. Te ostatnie były porównywalne w ich skutkach prawnych do przepisów WE i dyrektyw, tylko poważnie różniły się tym, że nie wywierały one bezpośredniego skutku. Dostępność decyzji i decyzje ramowe jako instrumenty prawne stanowiły znaczne ulepszenie w stosunku do sytuacji sprzed obowiązywania Traktatu z Amsterdamu, gdy instrumenty „miękkiego prawa" były często używane jako opcja dla państw członkowskich. Rada mogła się również zgodzić na konwencje, które jednak podlegały ratyfikacji przez państwa członkowskie, a procedury, które mogły trwać wiele lat, sprawiają, że konwencja była bardzo trudna do zastosowania.

Wszystkie te instrumenty były przedmiotem kontroli Europejskiego Trybunału Sprawiedliwości, ale zgodnie z tyt. VI TUE tylko sądy państwowe ostatniej instancji mogą starać się o wydanie orzeczenia Trybunału w sprawie pytań prejudycjalnych. Trybunał nie miał jurysdykcji nad ważnością lub proporcjonalnością środków egzekwowania prawa przez władze państw członkowskich, i gdy istniał spór dotyczący interpretacji środka UE, Trybunał mógł tylko orzekać w sytuacji, kiedy Rada nie rozwiązała problemu w ciągu sześciu miesięcy[402].

Instytucja wzmocnionej, ściślejszej współpracy nie została zdefiniowana w Traktacie o Unii Europejskiej na podstawie TWE. Przepisy ogólne regulujące tę instytucję zawarto w tytule VII Traktatu z Amsterdamu, a przepisy dotyczące wzmocnionej współpracy o charakterze policyjnym i sądowym w sprawach karnych umieszczono w art. 40–40b TUE. Ma to służyć wzmocnionej integracji tych państw, które są do tego przygotowane lub chcą do niej dążyć. Pozostałe państwa nie mogą stawać im na przeszkodzie.

Mimo braku wyraźnej definicji instytucji wzmocnionej współpracy można na podstawie postanowień TWE i TUE wywnioskować, że polega ona na intensywnej współpracy między sobą lub w szerszym zakresie niż pozostałe części państw członkowskich, przy czym współpraca ta wykorzystuje istniejące już, przewidziane w TUE instytucje, organy i procedury. Wzmocniona współpraca jest

wyjątkiem od zasady solidarności zawartej w art. 10 TWE, 2 TWE i 1 TUE, stanowiącej jeden z fundamentów prawa wspólnotowego[403].

Warunki wzmocnionej współpracy zostały zawarte w art. 40–40b TUE z poszanowaniem art. 43 i art. 44 TEU. Państwa członkowskie, które zamierzają ustanowić między sobą wzmocnioną współpracę, mogą korzystać z instytucji, procedur i mechanizmów przewidzianych niniejszym traktatem oraz Traktatem ustanawiającym Wspólnotę Europejską, pod warunkiem że współpraca ta m.in.[404]:

- szanuje kompetencje Wspólnoty Europejskiej oraz cele określone w niniejszym tytule,
- ma na celu umożliwienie Unii szybszego przekształcenia się w przestrzeń wolności, bezpieczeństwa i sprawiedliwości.

Zgodnie z art. 43 wzmocniona współpraca może zostać podjęta tylko w ostateczności, tzn. gdy wytyczone cele nie mogą być osiągnięte w drodze zwykłych procedur w rozsądnym terminie przez zastosowanie odpowiednich postanowień traktatów. Jest otwarta w stosunku do wszystkich państw członkowskich, co oznacza, że pozwala im przyłączyć się do współpracy w każdej chwili, jeśli zastosują się do decyzji podstawowej oraz decyzji już podjętych w ramach tej współpracy.

Warto zwrócić uwagę na zapis w art. 42 TUE. Jest to procedura przekazywania instrumentów z III do I filaru, czyli zmiany charakteru współpracy z międzyrządowej na ponadnarodową. Rada, stanowiąc jednomyślnie z inicjatywy Komisji lub państwa członkowskiego, po zasięgnięciu opinii Parlamentu Europejskiego może zdecydować, że działania w dziedzinach wskazanych w art. 29 podlegają tyt. IV TUE ustanawiającego Wspólnotę Europejską, i jednocześnie może określić warunki głosowania, które są z tym związane. Transfer kompetencji będzie prowadzić w rzeczywistości do zmiany TUE i TWUE ustanawiającego ogólną procedurę zmiany traktatów założycielskich. Mechanizm co prawda składa się z dwóch stadiów: unijnego i państwowego, różnica jednak tkwi w szybkości i rezygnacji z konferencji międzyrządowej przygotowującej zmiany w traktatach.

Artykuł 42 nie stawia żadnych dodatkowych warunków dotyczących materialnego zakresu stosowania mechanizmu. Przedmiotem może być każda dziedzina wskazana w art. 29, czyli również polityka antyterrorystyczna. W skrajnym przypadku do I filaru może zostać przekazana całość współpracy policyjnej i sądowej w sprawach karnych[405].

Traktat z Amsterdamu był pierwszym w historii Wspólnot Europejskich aktem prawnym, w którym państwa członkowskie uznały, że jedynym efektywnym sposobem zwalczania przestępczości zorganizowanej jest ich ściślejsza współpraca koncentrująca się na działaniach operacyjnych i administracyjnych. Traktat dopuszczał bowiem możliwość działania funkcjonariuszy właściwych służb danego państwa na terytorium innych państw UE[406].

4.2.1.3. Traktat z Nicei

Po podpisaniu Traktatu z Nicei 26 lutego 2001 r.[407] Rada Europejska przyjęła dwa ważne instrumenty: *Europejską strategię bezpieczeństwa* oraz dokument *Obrona europejska: konsultacje NATO/UE, planowanie i operacje*, pozwalające na rozpoczęcie prac cywilno-wojskowych oraz utworzenie centrum operacji[408]. Najistotniejsze zmiany, jakie ten traktat wprowadził w ramach III filaru, dotyczyły powołania Eurojustu[409], który miał być ośrodkiem współpracy organów sądowych państw członkowskich oraz określenia warunków nawiązywania wzmocnionej (ściślejszej) współpracy[410]. Jej celem miało być zapobieganie i zwalczanie m.in. zorganizowanej przestępczości oraz terroryzmu (znowelizowany art. 31 TUE). Traktat z Nicei uchylił art. 17 Traktatu o Unii Europejskiej w sprawie stosunków między Unią a UZE, a tym samym włączenie UZE zarządzaniem kryzysowym do Unii Europejskiej.

Ranga Eurojustu wzrosła po szczycie w Nicei w grudniu 2000 r. Jedną z najważniejszych decyzji zawartych w Traktacie z Nicei, dotyczącą współpracy w ramach III filaru, było włączenie do tyt. VI TUE postanowień dotyczących Eurojustu. Traktat wprowadza do art.

29 TUE odniesienie do Eurojustu jako organu umożliwiającego bliższą współpracę między organami sądowymi a innymi kompetentnymi władzami w państwach członkowskich[411]. Zasadnicza zmiana uzgodniona w Nicei dotyczy wspierania Eurojustu w przypadkach poważnych przestępstw transgranicznych oraz ułatwienia ścisłej współpracy między Eurojustem a Europejską Siecią Sądową, w szczególności w celu realizacji wniosków o ekstradycję (art. 31, ust. 2, lit. c TUE).

Eurojust współpracuje z Europolem, co wynika z art. 31 ust. 2 lit. b TUE i art. 26 ust. 1 decyzji ramowej Rady nr 2002/187/JHA. Posiada również osobowość prawną, a kontrolę nad ogólną działalnością Eurojustu w zakresie gromadzenia, przetwarzania i dysponowania danymi sprawuje Wspólny Organ Nadzorczy[412].

Konsekwencją przyjęcia tych decyzji były zmiany organizacyjne w III filarze UE. Zlikwidowano Grupy Kierownicze i utworzono trzy podstawowe piony współpracy. Grupy Robocze ds. Terroryzmu, Europolu oraz Systemu Informacji Schengen, które znalazły się w pionie współpracy policyjnej oraz celnej, zostały bezpośrednio podporządkowane Komitetowi Koordynacyjnemu[413].

Traktat z Nicei nie wprowadził żadnych zmian co do treści art. 30, 34 i 35 TUE. Z kolei na podstawie art. 31 wspólne działania w dziedzinie współpracy sądowej w sprawach karnych obejmują m.in.:

- ułatwianie i przyspieszanie współpracy między ministerstwami i organami sądowymi lub odpowiednimi organami państw członkowskich, w tym w miarę potrzeby współpracy za pośrednictwem Eurojustu w zakresie procedury sądowej i wykonywania orzeczeń;
- ułatwianie ekstradycji między państwami członkowskimi;
- zapewnianie w zakresie niezbędnym do usprawnienia tej współpracy zgodności norm stosowanych w państwach członkowskich;
- zapobieganie sporom o właściwość między państwami członkowskimi;
- stopniowe przyjmowanie środków ustanawiających minimalne normy dotyczące znamion przestępstw i kar w dziedzinach

przestępczości zorganizowanej, terroryzmu i nielegalnego handlu narkotykami.

W wyniku szybkiego rozwoju wymiaru sprawiedliwości i spraw wewnętrznych UE w latach 90. XX w. znacznie poprawiły się strukturalne podstawy do walki z terroryzmem na poziomie UE. Luźne międzyrządowe struktury TREVI zostały w pełni włączone w strukturę Rady z Wymiarem Sprawiedliwości i Spraw Wewnętrznych (JHA Council). Rada skupia przedstawicieli ministerstw spraw wewnętrznych i sprawiedliwości poszczególnych państw członkowskich i odpowiedzialnego członka Komisji Europejskiej. Dzieli wszelkie środki zwalczania terroryzmu z wymiarem sprawiedliwości i spraw wewnętrznych. Związane aspekty z WPZiB pozostawia się Radzie ds. Ogólnych, która skupia wokół siebie ministrów spraw zagranicznych. Ogólna koordynacja procesem podejmowania decyzji przebiega poniżej szczebla ministerialnego i formalnie należy do Komitetu Stałych Przedstawicieli (COREPER)[414], jednak w domenie wymiaru sprawiedliwości i spraw wewnętrznych COREPER zwykle odgrywa aktywną rolę tylko wtedy, gdy występują trudności w osiągnięciu porozumienia w wyspecjalizowanych komisjach Rady lub jeżeli istnieją zagadnienia przekrojowe, takie jak koordynacja między filarami bądź wykorzystanie środków z budżetu WE. W praktyce zatem istotną rolę w przygotowaniu decyzji ministerialnych na temat walki z terroryzmem odgrywał art. 36. Jest on podstawą prawną funkcjonowania dobrze zakorzenionego już od TUE Komitetu Koordynacyjnego, którego zasadniczym zadaniem jest koordynacja zadań państw członkowskich w ramach dawnego III filaru. Tym samym pomaga w realizacji zobowiązania wyrażonego w art. 34 ust. 1 TUE[415]. Komitet ma możliwość wpływania na kierunki rozwoju i pomaga w przygotowywaniu prac Rady, gdy ma się ona zająć współpracą policyjną i sądową w sprawach karnych[416]. W skład Komitetu (CATS) wchodzą wyżsi urzędnicy państwowi i Komisja zajmująca się współpracą sądową i policyjną. Wydaje on instrukcje Radzie Grupy Roboczej ds. Terroryzmu (WPT), która skupia państwowych i europejskich urzędników Komisji, zajmujących się

zwalczaniem terroryzmu w kontekście III filaru. WPT jest odpowiedzialna za opracowanie szczegółów walki z terroryzmem, a problemy bardziej szczegółowe, odnoszące się do współpracy policyjnej oraz sądowej, zostały przypisane innym wyspecjalizowanym grupom roboczym Rady.

Drugą ważną zmianą była kwestia procedury wzmocnionej współpracy. Po wprowadzeniu przez TA możliwości nawiązywania wzmocnionej współpracy nie doszło do zwieńczonego powodzeniem wykorzystania tej instytucji, a w perspektywie rozszerzenia Unii ukształtowały się dwie przeciwstawne grupy państw. Jedną reprezentowały państwa wysoko rozwinięte, obawiające się, że w wyniku rozszerzenia UE nastąpi blokada w podejmowaniu decyzji, czego dowodem były daleko posunięte złagodzenia przepisów dotyczących głosowania. Drugą grupę stanowiły w dużej mierze państwa kandydujące, zmierzające do utrzymania dotychczasowego kształtu przepisów, ponieważ obawiały się, że tak skonstruowana procedura zostanie wykorzystana jako mechanizm wykluczenia skierowany przeciwko nowym członkom, a w dalszej konsekwencji do dyferencjacji wspólnotowego porządku prawnego.

Traktat z Nicei uregulował ogólne warunki wzmocnionej współpracy. Istotna zmiana polega na tym, że zgodnie z TN powinna być ona nakierowana na wspieranie celów nie tylko samej Unii, ale także Wspólnoty oraz wzmocnienie procesu ich integracji. Ważne znaczenie miało też wprowadzenie dolnej granicy dotyczącej liczby państw podejmujących wzmocnioną współpracę. W TA musiała to być większość państw. W miejsce dotychczasowego zapisu o wymogu informowania przez Radę i Komisję Parlamentu o rozwoju wzmocnionej współpracy wprowadzono zapis o współpracy Rady i Komisji, który ma na celu zapewnienie spójności działań podjętych w ramach wzmocnionej współpracy oraz ich zgodności z politykami UE i Wspólnot.

W części ujednolicono procedurę podjęcia wzmocnionej współpracy w obszarze I i III filaru. W myśl art. 40a ust. 1 państwa członkowskie zamierzające ustanowić między sobą wzmocnioną współpracę mogą:

- na mocy art. 40 skierować wniosek do Komisji, która może przedłożyć Radzie odpowiednią propozycję;
- Komisja może zwrócić się ze stosowną propozycją do Rady, a jeżeli Komisja rozpatrzy wniosek negatywnie, zawiadamia o tym zainteresowane państwa członkowskie, podając uzasadnienie;
- państwa członkowskie mogą same zwrócić się do Rady w celu uzyskania upoważnienia do ustanowienia wzmocnionej współpracy;
- po konsultacji z Parlamentem Europejskim Rada większością kwalifikowaną udziela upoważnienia do podjęcia wzmocnionej współpracy.

Każde państwo członkowskie może przekazać sporną kwestię pod dyskusję Rady Europejskiej, podczas gdy w myśl zapisów Traktatu z Amsterdamu mogła to uczynić tylko Rada UE. Możliwość blokady decyzji przez jedno państwo członkowskie ze względu na ważny interes narodowy zostało znacznie utrudnione.

Zdecydowano o jednolitej procedurze przystąpienia do wzmocnionej współpracy w obszarze II i III filaru. Odbywa się ono na mocy art. 40b TUE w ten sposób, że każde państwo członkowskie, które pragnie uczestniczyć we wzmocnionej współpracy ustanowionej na mocy art. 40a, notyfikuje swój zamiar Radzie i Komisji, która przedkłada Radzie opinię w terminie trzech miesięcy od otrzymania tej notyfikacji. Rada podejmuje decyzję w sprawie wniosku w terminie czterech miesięcy od otrzymania notyfikacji. Decyzję uważa się za przyjętą, chyba że Rada, stanowiąc większością kwalifikowaną, w tym samym terminie zadecyduje o jej wstrzymaniu. W ostatnim przypadku Rada uzasadnia swoją decyzję i określa ostateczny termin jej ponownego rozpatrzenia.

Funkcjonowanie wzmocnionej współpracy polega na tym, że w celu podjęcia aktów i decyzji potrzebnych do jej realizacji przewidziane jest odpowiednie stosowanie przepisów UE i TWE. Uchwały Rady podejmują tylko przedstawiciele państw biorących udział w bliższej współpracy, natomiast większość kwalifikowana oznacza taki sam udział głosów ważonych oraz taki sam udział liczby odnośnych członków Rady określony w art. 205 ust. 2 TWE[417].

Ważne postanowienia zostały zawarte w art. 44 ust. 2 TN, ponieważ wynika z niego, że akty i decyzje przyjęte w ramach współpracy są wiążące i mają bezpośrednie zastosowanie do tych państw członkowskich, które w niej uczestniczą. Tym samym przyznano decyzjom podjętym w ramach wzmocnionej (ściślejszej) współpracy większą moc niż aktom prawnym III filara, co do których wyraźnie zastrzeżono, że nie mają charakteru bezpośredniego[418].

4.2.1.4. Traktat z Lizbony

W perspektywie europejskiej wymiar bezpieczeństwa cybernetycznego jest obecnie jednym z najważniejsze priorytetów politycznych UE, przy czym jego elementy można znaleźć w ramach innych polityk UE[419]. Dla wielu państw wyzwanie stanowi zdefiniowanie polityki cyberbezpieczeństwa, która jest złożonym i wielowarstwowym zjawiskiem i w tym kontekście jest wyraźnie powiązana z wieloma innymi politykami. Ponadto, przez wdrażanie wielu tematów, wymagań definicyjnych, klasyfikacji, standardów do debaty publicznej oraz certyfikacji i innych procedur, UE wpływa i kształtuje politykę cyberbezpieczeństwa państw członkowskich. Istotne są także mniej techniczne tematy, które obejmują kształtowanie świadomości społecznej w zakresie cyberzagrożeń, budowanie umiejętności i wiedzy przez edukację i wymianę informacji.

Jako regionalny sojusz gospodarczy i polityczny UE dąży do realizacji wspólnych interesów 28 państw członkowskich (po brexicie – 27). Fundamentem polityki UE jest rozwój oraz stabilne funkcjonowanie jednolitego rynku, czyli swobodny przepływ towarów, usług, kapitału i ludzi, określany również jako rynek wewnętrzny. Pojawia się jednak poważny problem, którym może być możliwość wystąpienia paraliżu funkcjonowania jednolitego rynku, czego przykładem były zdarzenia wynikające z ataków szkodliwych programów, np. WannaCry czy NotPetya w 2017 r., które doprowadziły do wielu zakłóceń działalności podmiotów międzynarodowych[420].

Należy podkreślić, że w przypadku państw europejskich terroryzm, a tym samym cyberterroryzm miał początkowo przede wszystkim charakter wewnętrzny. To spowodowało następstwa dwojakiego rodzaju. Państwa uznawały i w dużej mierze nadal uznają, że przeciwdziałanie terroryzmowi to zagadnienie należące do ich wyłącznej kompetencji. Współpracę międzynarodową w tym zakresie postrzegają jako konieczną, ale stanowiącą jedynie uzupełnienie i poszerzanie zdolności do walki z terroryzmem[421].

Wraz z wprowadzeniem tyt. VI TUE przez Traktat z Maastricht działania UE zostały po raz pierwszy wyposażone w podstawę prawną, w której ramach wzmocniono je i rozszerzono przez Traktat z Amsterdamu. Jednym z najważniejszych przepisów był art. 2 TUE, który przewidywał utrzymanie i rozwój UE jako przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Bezpieczeństwo wewnętrzne leży u jego podstaw. W art. 29 Traktatu o Unii Europejskiej zagwarantowano „obywatelom wysoki poziom bezpieczeństwa". Cel ten został powtórzony niemal identycznie w art. 61e TUE, co oznaczało, że Unii udzielono mandatu zaufania jako dostawcy bezpieczeństwa wewnętrznego. Z kolei w art. 29 ust. 2 TUE wymieniono terroryzm jako formę przestępczości, przeciwko której powinny być skierowane szczególne działania[422]. W związku z tym UE wyznaczyła siedem celów strategicznych dotyczących polityki antyterrorystycznej[423]. Patrząc z perspektywy czasu na powolny rozwój polityki antyterrorystycznej, a wraz z nią polityki ochrony cyberprzestrzeni, należy również odnieść te kwestie do działań polityki bezpieczeństwa UE, która ze względu na ówczesny rozwój technologii nie rozumiała do końca obszaru zagrożenia.

Z obecnego brzmienia TUE wyłączone zostały art. 29–39 TUE, które zastąpiono postanowieniami części trzeciej tyt. V TFUE (art. 67–89 TFUE), a zamiast art. 40–40b TUE wprowadzono przepis art. 20 TFUE regulujący tę problematykę. Zmiany dokonane przez Traktat z Lizbony w ramach wymienionych wcześniej polityk mają charakter systemowy, a nie merytoryczny. Należy również zauważyć, że dotychczasowe polityki znajdujące się w ramach dawnego III filaru stały się elementem kształtowania obecnej polityki

bezpieczeństwa UE. Wynika to z rosnącego zagrożenia ze strony organizacji terrorystycznych i fundamentalistycznych. Polityki te zostały wyposażone w jednakowy katalog instrumentów prawnych i niemal identyczne kompetencje instytucji w tym zakresie.

Umiejscowienie w art. 2 ust. 2 TUE na drugim miejscu celu, jakim jest zapewnienie obywatelom przestrzeni wolności, bezpieczeństwa i sprawiedliwości, tuż po celu, jakim jest wspieranie pokoju, jego wartości i dobrobytu wśród narodów, podkreśla również znaczenie, jakie państwa członkowskie nadają współpracy w tym obszarze. Wskazuje to również na kolejny etap w rozwoju wspólnego działania w tej materii obserwowany od lat 70. XX w.[424]

Dotychczasowe przepisy dotyczące wzmocnionej współpracy (art. 27a–27e, 40–40b i 43–45 TUE oraz d. art. 11 i 11a TWE) zostały zastąpione w Traktacie z Lizbony art. 10 (art. 20 TFUE) stanowiącym, że państwa członkowskie, które pragną ustanowić między sobą wzmocnioną współpracę[425] w ramach kompetencji niewyłącznych Unii, mogą korzystać w tym celu z jej instytucji i wykonywać te kompetencje, stosując odpowiednie postanowienia traktatów, z zastrzeżeniem ograniczeń oraz zgodnie z procedurą określoną w niniejszym artykule i w art. 326–334 TFUE. W ten sposób zagwarantowano wsparcie realizacji celów Unii, ochronę jej interesów oraz wzmocnienie procesu jej integracji. Tego typu współpraca jest dostępna dla wszystkich państw członkowskich w dowolnym czasie, zgodnie z art. 328 Traktatu o funkcjonowaniu Unii Europejskiej.

Traktat podkreśla znaczenie i zasadnicze kompetencje państw członkowskich w zakresie działań zewnętrznych. Poszerza dotychczasowe kompetencje i uprawnienia UE umożliwiające większe przeciwdziałanie zagrożeniom cyberterrorystycznym i terrorystycznym. Stosownie do art. 21 TUE i n. (art. 10a TL) „Unia określa i prowadzi wspólne polityki i działania oraz dąży do zapewnienia wysokiego stopnia współpracy we wszelkich dziedzinach stosunków międzynarodowych w celu m.in. utrzymania pokoju, zapobiegania konfliktom i umacniania bezpieczeństwa międzynarodowego, a także w celu wspierania trwałego rozwoju

gospodarczego i społecznego". Kompetencje Unii w zakresie wspólnej polityki zagranicznej i bezpieczeństwa obejmują wszelkie dziedziny polityki zagranicznej i kwestie dotyczące bezpieczeństwa Unii, w tym stopniowe określanie wspólnej polityki obronnej. Zgodnie z art. 28b ust. 1 Traktatu z Lizbony (art. 43 TUE) Unia może powoływać misje humanitarne i ratunkowe, misje wojskowego doradztwa i wsparcia, misje zapobiegania konfliktom i utrzymywania pokoju, misje zbrojne służące zarządzaniu kryzysowemu, w tym misje przywracania pokoju i operacje stabilizacji sytuacji po zakończeniu konfliktów. Działania te mogą się przyczyniać do walki z cyberterroryzmem i terroryzmem, w tym poprzez wspieranie państw trzecich w zwalczaniu terroryzmu na ich terytoriach. Terroryzm został uznany również za przestępstwo transgraniczne.

Traktat z Lizbony w art. 18 TUE wprowadził stanowisko wysokiego przedstawiciela ds. zagranicznych i polityki bezpieczeństwa w miejsce ministra spraw zagranicznych. Stosownie do tego artykułu wysoki przedstawiciel ds. zagranicznych i polityki bezpieczeństwa jest powoływany przez Radę Europejską stanowiącą większością kwalifikowaną, za zgodą przewodniczącego Komisji. Pełni on jednocześnie funkcję przewodniczącego Komisji Europejskiej. Wysoki przedstawiciel przewodniczy z urzędu jednemu ze składów Rady, którym jest Rada ds. Zagranicznych (ust. 3 art. 18 TUE). Prowadzi WPZiB, w tym Wspólną Politykę Bezpieczeństwa i Obrony Unii, przedstawiając propozycje dotyczące opracowania tej polityki i ją realizując. Jako członek Komisji Europejskiej odpowiada za jej obowiązki w obszarze stosunków zewnętrznych i koordynację innych aspektów działań zewnętrznych Unii, podlega procedurom regulującym funkcjonowanie Komisji, o ile nie jest to sprzeczne z jego szczególnymi zadaniami (ust. 4 art. 18 TUE). Wpłynęło to na wzmocnienie możliwości decyzyjnych UE w polityce zagranicznej[426].

Traktat z Lizbony dokonuje rozdziału zadań między UE a państwa w sposób o wiele bardziej precyzyjny niż dawne przepisy. Już w art. 3a TUE (nowy art. 4) doprecyzowano, że UE szanuje podstawowe

funkcje państwa. Koreluje to częściowo z postanowieniami art. 67 TFUE.

Zgodnie z obecnym art. 75 Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej polityka antyterrorystyczna i cyberbezpieczeństwa jest oparta na zasadzie współdecydowania. Podstawą prawną procedury współdecydowania (kodecyzji) jest art. 251 TWE. Organami współdecydującymi o przyjęciu lub odrzuceniu aktu prawnego są Rada i Parlament Europejski, inicjatywa ustawodawcza natomiast należy do Komisji[427]. Głównym założeniem tej zasady jest uniknięcie podejmowania decyzji[428] bez uzgodnienia wspólnego stanowiska między tymi dwoma ciałami a Komisją Europejską[429]. Takie rozwiązanie okazało się sukcesem w przypadku rozbieżnych często stanowisk poszczególnych grup interesów pojawiających się na poszczególnych etapach procesu legislacyjnego[430].

Artykuł 67 TFUE to dawny art. 61 TWE i art. 29 TUE. Stanowi on, że UE jest przestrzenią wolności, bezpieczeństwa i sprawiedliwości w poszanowaniu praw podstawowych oraz różnych systemów i tradycji prawnych państw członkowskich. Jeżeli wymaga tego realizacja celów, o których mowa w odniesieniu do przeciwdziałania terroryzmowi i działalności powiązanej oraz zwalczaniu tych zjawisk, to Parlament Europejski i Rada, stanowiąc w drodze rozporządzeń zgodnie ze zwykłą procedurą prawodawczą, określają ramy środków administracyjnych dotyczących przepływu kapitału i płatności, takich jak zamrożenie funduszy, aktywów finansowych lub zysków z działalności gospodarczej, które należą do osób fizycznych lub prawnych, grup lub podmiotów innych niż państwa, są w ich posiadaniu lub dyspozycji (obecny art. 75 TFUE[431]).

Nowością okazał się art. 68 TFUE, na podstawie którego Rada Europejska określa strategiczne wytyczne planowania prawodawczego i operacyjnego w przestrzeni wolności, bezpieczeństwa i sprawiedliwości. W myśl art. 71 TFUE pozostawiono w ramach Rady stały komitet ds. zapewnienia, wspierania i wzmacniania współpracy operacyjnej wewnątrz Unii w zakresie bezpieczeństwa wewnętrznego[432].

Obecne art. 82–83 i 85 są poszerzeniem dawnych art. 29 i 31 TUE. Na podstawie art. 82 ust. 1 TFUE można łatwo zauważyć, że podstawowym celem współpracy sądowej w sprawach karnych w UE jest wzajemne uznawanie wyroków i orzeczeń sądowych oraz zbliżanie przepisów ustawowych i wykonawczych państw członkowskich w następujących dziedzinach: terroryzm, cyberterroryzm, handel ludźmi oraz seksualne wykorzystywanie kobiet i dzieci, nielegalny handel narkotykami, nielegalny handel bronią, pranie pieniędzy, korupcja, fałszowanie środków płatniczych, przestępczość komputerowa i przestępczość zorganizowana[433]. Należy przyjąć, że powodem wyszczególnienia tych przestępstw były skutki wynikające z ich rodzaju lub ze szczególnej potrzeby wspólnego ich zwalczania. Podobnie jak w Traktacie z Maastricht, jest to katalog zamknięty[434].

Istotne było wprowadzenie w art. 82 ust. 2 TL możliwości harmonizacji przepisów z zakresu prawodawstwa karnego przez normy minimalne o wymiarze transgranicznym, z uwzględnieniem różnic między tradycjami a systemami prawnymi poszczególnych państw członkowskich.

Państwa, niezależnie od minimalnych standardów przewidzianych w normach, mogą utrzymywać lub ustanawiać wyższy poziom ochrony osób. Istotną zmianą w porównaniu z obecnym stanem prawnym jest zmiana procedury przyjmowania tych norm minimalnych – na mocy TFUE są one ustalane w formie dyrektyw przyjmowanych w zwykłej procedurze prawodawczej przez Parlament Europejski i Radę UE[435]. W konsekwencji od momentu wejścia w życie TL zasadą stała się harmonizacja dyrektyw przyjmowanych przez Radę kwalifikowaną większością głosów w zwykłej procedurze prawodawczej, gdy w poprzednim stanie prawnym harmonizacja prawa karnego odbywała się w drodze decyzji ramowych przyjmowanych jednomyślnie. Trzeba dodać, że zwykła procedura prawodawcza przewidziana w TL jest wzorowana na dotychczasowej procedurze współdecydowania (określonej w d. art. 251 TWE), która gwarantuje Parlamentowi Europejskiemu istotny wpływ na kształt przyjmowanego aktu prawnego[436].

Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą prawodawczą, przyjmują środki mające na celu:

- ustanowienie zasad i procedur zapewniających uznawanie w całej Unii wszystkich form wyroków i orzeczeń sądowych,
- zapobieganie sporom o właściwość między państwami członkowskimi i ich rozstrzyganie,
- wspieranie szkolenia sędziów i innych pracowników wymiaru sprawiedliwości,
- ułatwianie współpracy między organami sądowymi lub równoważnymi organami państw członkowskich w ramach ścigania karnego i wykonywania orzeczeń.

Przyjęcie norm minimalnych w dziedzinach innych niż wskazane w tym przepisie wymaga uprzedniej zgody Rady. Zgodnie z art. 83 ust. 1 akapit 3 TFUE, w zależności od rozwoju przestępczości Rada, działając jednomyślnie i po uzyskaniu zgody Parlamentu Europejskiego, może przyjąć decyzję określającą inne dziedziny przestępczości spełniające kryteria, o których mowa w tym ustępie. Ta radykalna zmiana po analizie okazuje się mniej przełomowa. Wprowadzenie przyjmowania dyrektyw kwalifikowaną większością głosów przez Radę zostało ograniczone do tych obszarów, które już poddano harmonizacji w drodze decyzji ramowych, czyli aktów prawnych III filara. Ewentualna modyfikacja przepisów przyjętych lub uzgodnionych decyzji ramowych będzie się odbywała już na podstawie TFUE i doprowadzi do przekształcenia tych aktów w dyrektywy (ze wszystkimi konsekwencjami instytucjonalnymi i systemowymi tej zmiany)[437].

Jeżeli zbliżanie przepisów ustawowych i wykonawczych państw członkowskich w sprawach karnych okaże się niezbędne w celu zapewnienia skutecznego wprowadzania w życie polityki Unii w dziedzinie, która stała się przedmiotem środków harmonizujących, zgodnie z art. 83 ust. 2 TFUE dyrektywy mogą ustanowić normy minimalne, odnoszące się do określania przestępstw oraz kar w danej dziedzinie. Dyrektywy te przyjmuje się zgodnie ze zwykłą lub specjalną procedurą prawodawczą, taką samą jak procedura

stosowana do przyjmowania stosownych środków harmonizujących[438].

Gdyby państwa członkowskie miały rozszerzyć zakres harmonizacji prawa karnego materialnego – zgodnie z przytoczonym wcześniej przepisem – konieczna byłaby jednomyślna decyzja Rady za zgodą Parlamentu Europejskiego. Rozwiązanie to z jednej strony chroni interes poszczególnych państw członkowskich, które mogą się w ten sposób sprzeciwiać rozszerzeniu zakresu harmonizacji, z drugiej – jest dowodem wolno postępującej harmonizacji w tym zakresie. W tym kontekście pojawiają się wątpliwości, czy decyzja podjęta na podstawie art. 83 ust. 1 akapit 3 TFUE powinna być traktowana jako akt prawa konstytucyjnego UE wyłączony spod zakresu kognicji ETS, czy też jak każdy akt prawa pochodnego UE. Należy też się zastanowić nad rolą parlamentów państwowych. Przy przyjmowaniu przez Radę decyzji na podstawie art. 83 ust. 1 akapit 3 TFUE będą wykorzystywane przepisy protokołu w sprawie stosowania zasad pomocniczości i proporcjonalności. Chodzi w szczególności o procedurę zawartą w art. 7 tego protokołu, wskazującą, że jeżeli określona liczba parlamentów narodowych przedstawi uzasadnione opinie o niezgodności projektu aktu prawodawczego z zasadą pomocniczości, musi to skłonić organ, który projekt przedstawił, do ponownej jego analizy. Procedura ta może stanowić dla parlamentów narodowych mocny instrument w dziedzinie PWBiS[439].

Jeżeli incydent nosi znamiona szpiegostwa cybernetycznego lub ataku inicjowanego przez państwo bądź ma wpływ na bezpieczeństwo państwa, krajowe organy bezpieczeństwa i obrony ostrzegają swoich odpowiedników, że są celem ataku, by mogli się odpowiednio bronić. Zostaną wówczas uruchomione mechanizmy wczesnego ostrzegania, a w razie konieczności także procedura zarządzania kryzysowego i inne. Szczególnie poważny incydent lub atak w zakresie bezpieczeństwa cybernetycznego może stanowić wystarczającą podstawę do tego, by państwo członkowskie powołało się na klauzulę solidarności UE (art. 222 TFUE)[440]. Jeżeli incydent wydaje się prowadzić do naruszenia danych osobowych, należy

powiadomić krajowe organy ds. ochrony danych lub krajowy organ regulacyjny, zgodnie z dyrektywą 2002/58/WE. W przypadku wystąpienia incydentów i ataków cybernetycznych przydatne będą sieci kontaktów i wsparcie ze strony partnerów międzynarodowych, które może obejmować zastosowanie środków technicznych ograniczających wpływ incydentu, prowadzenie dochodzeń oraz uruchomienie mechanizmów reagowania w sytuacjach kryzysowych.

W myśl art. 85 TFUE współpraca w sprawach karnych ma być uzupełniona działalnością Eurojustu, a w przyszłości Prokuratury Europejskiej. Zadaniem Eurojustu[441] jest wspieranie oraz wzmacnianie koordynacji i współpracy między państwowymi organami śledczymi a organami ścigania w odniesieniu do poważnej przestępczości, która dotyka dwóch lub więcej państw lub wymaga wspólnego ścigania na podstawie przeprowadzanych operacji i informacji dostarczanych przez organy państw członkowskich i Europol.

Na podstawie art. 86 TFUE za szczególny rodzaj przestępstw uznano przestępstwa przeciwko interesom finansowym Unii, w tym terroryzm finansowy. Prokuratura Europejska jest właściwa do wnoszenia przed właściwe sądy państw członkowskich publicznego oskarżenia dotyczącego tych przestępstw. Rada stanowi jednomyślnie po uzyskaniu zgody Parlamentu Europejskiego. W przypadku braku jednomyślności grupa co najmniej dziewięciu państw członkowskich może wystąpić z wnioskiem o przekazanie projektu rozporządzenia Radzie Europejskiej, a wówczas procedura w Radzie zostaje zawieszona. Po przeprowadzeniu dyskusji i w przypadku konsensusu Rada Europejska w terminie czterech miesięcy od daty zawieszenia odsyła projekt Radzie do przyjęcia. W takim samym terminie, w razie braku porozumienia i w sytuacji, gdy co najmniej dziewięć państw członkowskich zamierza ustanowić wzmocnioną współpracę na podstawie danego projektu rozporządzenia, informują one o tym Parlament Europejski, Radę i Komisję. W takim przypadku uznaje się, że upoważnienie do podjęcia wzmocnionej współpracy, o którym mowa w art. 20 ust. 2

TFUE i w art. 329 ust. 1 niniejszego traktatu, zostało udzielone i stosuje się postanowienia w sprawie wzmocnionej współpracy[442].

W myśl art. 87 ust. 1 TFUE (dawny art. 30 TUE) Unia ma za zadanie rozwijać współpracę policyjną obejmującą wszystkie właściwe organy państw unijnych, w tym służby policji, służby celne oraz inne organy ścigania wyspecjalizowane w zapobieganiu przestępstwom lub ich wykrywaniu i ściganiu. Do celów ust. 1 Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą prawodawczą, mogą ustanawiać środki dotyczące:

- gromadzenia, przechowywania, przetwarzania, analizowania i wymiany istotnych informacji,
- wspierania szkolenia pracowników oraz współpracy w zakresie wymiany pracowników oraz wyposażenia i badań w dziedzinie kryminalistyki,
- wspólnych technik śledczych dotyczących wykrywania poważnych form przestępczości zorganizowanej.

Z kolei zgodnie z art. 88 ust. 1 TFUE zadaniem Europolu[443] jest wspieranie i wzmacnianie działań organów policyjnych i innych organów ścigania państw unijnych, jak również ich współpracy w zapobieganiu i zwalczaniu poważnej przestępczości dotykającej dwóch lub więcej państw członkowskich, terroryzmu oraz form przestępczości naruszających wspólny interes objęty polityką Unii. Wszelkie działania operacyjne Europolu zgodnie z ust. 3 powyższego artykułu są prowadzone w powiązaniu i w porozumieniu z organami państwa członkowskiego, którego terytorium dotyczą. Stosowanie środków przymusu należy do wyłącznej kompetencji właściwych organów państwowych.

Zgodnie z art. 89 TFUE Rada określa jednomyślnie, po konsultacji z Parlamentem Europejskim, warunki i granice, w jakich właściwe organy państw członkowskich, w sytuacjach przewidzianych w art. 82 i art. 87 mogą podejmować działania na terytorium innego państwa członkowskiego w powiązaniu i w porozumieniu z organami tego państwa[444]. Jeżeli incydent nosi znamiona szpiegostwa lub ataku inicjowanego przez państwo trzecie albo ma wpływ na

bezpieczeństwo państwa członkowskiego UE, to państwowe organy bezpieczeństwa i obrony mogą na podstawie art. 222 TFUE ubiegać się o uznanie go za szczególnie poważny i włączyć zastosowanie tzw. klauzuli solidarności.

Mimo formalnych ograniczeń możliwe jest jednak znalezienie w traktatach UE podstawy do stanowienia prawa na poziomie Unii w zakresie bezpieczeństwa cybernetycznego odnoszącego się do funkcjonowania gospodarki. Unia Europejska ma w szczególności silny mandat na jednolitym rynku oraz w sieci transeuropejskiej, co zostało potwierdzone w Traktacie o funkcjonowaniu Unii Europejskiej w art. 114 i art. 172[445]. Ponadto możliwość działania legislacyjnego istnieje w sektorach gospodarczych, takich jak energia, zgodnie z art. 194 TFUE[446], czy transport – art. 90 TFUE[447], a także współpraca administracyjna w zakresie przestrzeni wolności, bezpieczeństwa i sprawiedliwości – art. 74 TFUE[448].

Należy również zwrócić uwagę na fakt, że na politykę krajową może mieć wpływ dostosowanie państwa do miękkich, nielegislacyjnych inicjatyw politycznych UE. Mniejsze koalicje państw członkowskich mogą również tworzyć pewne normy w ramach współpracy w celu dostosowania swoich polityk w wymiarze regionalnym. W ten sposób można także budować sojusze, aby kształtować politykę UE.

4.2.2. PRAWO WTÓRNE UNII EUROPEJSKIEJ WOBEC CYBERTERRORYZMU

Na poziomie prawa wtórnego Unii Europejskiej początki regulacji dotyczących bezpieczeństwa w sektorze informatycznym zostały zawarte w następujących aktach prawnych:

- dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[449], która została uchwalona w celu stworzenia generalnych ram ochrony danych osobowych w EWG;

- dyrektywa 2000/31/WE w sprawie handlu elektronicznego (dyrektywa o handlu elektronicznym), która ma na celu usunięcie przeszkód w transgranicznym świadczeniu usług online na rynku wewnętrznym. Artykuły 12–14 dyrektywy Departamentu tematycznego ds. praw obywatelskich i spraw konstytucyjnych ustanawiają precyzyjnie określone ograniczenia odpowiedzialności usługodawców będących pośrednikami, którzy oferują jedynie przekaz, buforowanie i hosting[450];
- dyrektywa 2002/20/WE Parlamentu Europejskiego i Rady z 7 marca 2002 r. w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej (dyrektywa o zezwoleniach)[451] określa zasady i warunki udzielania zezwoleń na udostępnienie sieci oraz świadczenie usług łączności elektronicznej. Do wymogów, jakie mogą być związane z uzyskaniem ogólnego zezwolenia, należą obowiązki dotyczące zapewnienia bezpieczeństwa sieci i świadczonych usług, w tym obowiązek utrzymania integralności sieci łączności powszechnej przez zapewnienie warunków mających zapobiegać zaburzeniom elektromagnetycznym między sieciami łączności elektronicznej lub usługami oraz obowiązek zabezpieczenia sieci publicznej przed dostępem podmiotów nieuprawnionych;
- dyrektywa 2002/22/WE Parlamentu Europejskiego i Rady z 7 marca 2002 r. w sprawie usługi powszechnej i związanej z sieciami i usługami łączności elektronicznej praw użytkowników (dyrektywa o usłudze powszechnej)[452], zgodnie z art. 23 tej dyrektywy państwa członkowskie zobowiązane są do podjęcia koniecznych środków w celu zapewnienia integralności stacjonarnej publicznej sieci telefonicznej oraz, w przypadku załamania sieci w wyniku katastrofy lub w przypadku działania siły wyższej, dostępności usług stacjonarnej publicznej sieci telefonicznej i publicznie dostępnych usług telefonicznych. Podejmowane przez przedsiębiorstwa świadczące stacjonarne publicznie dostępne usługi telefoniczne w tym zakresie kroki

powinny się mieścić w granicach rozsądku w celu zapewnienia nieprzerwanego dostępu do służb ratunkowych;

- dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady Unii Europejskiej z 12 lipca 2002 r. o prywatności i łączności elektronicznej dotyczącej m.in. bezpieczeństwa publicznych sieci łączności elektronicznej[453]. Dyrektywa 2002/58/WE o ochronie danych w sektorze komunikacji elektronicznej ma zapewnić zastosowanie tych zasad w dynamicznie rozwijającym się sektorze komunikacji elektronicznej;
- decyzja ramowa 2005/222/WSiSW Rady z 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[454];
- dyrektywa 2008/114/WE w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony[455] dotyczy wymiany informacji w sektorze energetycznym w ramach EIK, która powinna odbywać się w warunkach zaufania i cyberbezpieczeństwa, aby firmy i organizacje miały pewność, że dotyczące ich dane wymagające szczególnej ochrony i dane poufne są odpowiednio chronione;
- dyrektywa nr 2011/93/UE z 13 grudnia 2011 r.[456] dotycząca zwalczania wykorzystywania seksualnego dzieci, w tym pornografii dziecięcej;
- dyrektywa 2013/40/UE[457] z 12 sierpnia 2013 r., której celem jest usprawnienie współpracy właściwych organów państw członkowskich w dziedzinie ataków na systemy informatyczne oraz ustanowienie minimalnych norm dotyczących określania przestępstw i kar w dziedzinie ataków na systemy informatyczne;
- dyrektywa 2014/41/UE Parlamentu Europejskiego i Rady z 3 kwietnia 2014 r.[458] dotycząca europejskiego nakazu dochodzeniowego (END);
- rozporządzenie GDRP/RODO 2016/679 jest aktem ujednolicającym przepisy prawa unijnego dotyczące ochrony danych osobowych i tożsamości;
- dyrektywa 2016/1148 NIS jest pierwszym aktem prawa UE w zakresie cyberbezpieczeństwa, wprowadzającym regulacje

międzysektorowe.

Dyrektywa 95/46/WE określiła wszystkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, przetwarzaniem zaś określiła wszystkie operacje dokonywane na danych osobowych, wymieniając je. Wprowadziła katalog minimalnych praw służących osobom, których dane są zbierane. Ich naruszenie miałoby skutkować możliwością dochodzenia tych praw na drodze sądowej. Dopuszczalność przetwarzania danych została uzależniona od woli (zgody) osoby, której dotyczą dane osobowe, przewidziała jednak zamknięty katalog sytuacji, gdy jest to możliwe bez takiej zgody. Dyrektywa wyodrębnia grupę danych osobowych tzw. sensytywnych. W przypadku ich przetwarzania wymagana jest zgoda wyrażona na piśmie. Odrębnie potraktowano też dane dotyczące „skazań kryminalnych", które mogą być przetwarzane jedynie przez podmioty publiczne. Sprecyzowano, kiedy możliwe jest odstępstwo od zasady zakazu przetwarzania takich danych. Jednocześnie dane te mogą być wykorzystywane wyłącznie zgodnie z celem, w którym zostały zgromadzone. Dyrektywa wprowadziła obowiązek informowania osoby o zasadach przetwarzania jej danych przed ich zgromadzeniem. Osoba ta może się sprzeciwić przetwarzaniu swoich danych, jeśli tylko posiada stosowne uzasadnienie. Każda osoba, której dane znalazły się już w zbiorze, ma prawo dowiedzieć się o zasadach ich przetwarzania, począwszy od możliwości ustalenia informacji o administratorze, skończywszy na ustaleniu treści tych danych. Dyrektywa wprowadziła też prawo kontroli danych osobowych przez osobę, której one dotyczą, w tym prawo wniesienia sprzeciwu przeciwko przetwarzaniu danych. Osobie, która poniosła szkodę wynikającą z przetwarzania danych niezgodnie z dyrektywą, przysługuje odszkodowanie. Jedną z najważniejszych regulacji wprowadzonych tą dyrektywą jest kwestia przekazywania danych osobowych do krajów trzecich (jest to możliwe, gdy kraj docelowy zapewnia odpowiedni poziom ochrony takich danych).

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady Unii Europejskiej z 12 lipca 2002 r. o prywatności i łączności

elektronicznej dotyczącej m.in. bezpieczeństwa publicznych sieci łączności elektronicznej[459] dotyczy przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej. Jest ona uszczegółowieniem dyrektywy 95/46/WE, która została uchwalona w celu stworzenia jedynie generalnych ram ochrony danych osobowych we EWG[460]. Przyjęcie dyrektywy było odpowiedzią Unii Europejskiej na wzrastający zasięg sieci cyfrowej telekomunikacji, szybkie pojawianie się nowych usług telekomunikacyjnych oraz wzrost związanego z tym zagrożenia prywatności i wolności użytkowników. Możliwość łatwego i systematycznego komputerowego zapisywania oraz przetwarzania danych dotyczących ruchu, czyli wszelkich danych przetwarzanych do celów przekazywania komunikatu w sieci łączności elektronicznej lub naliczania opłat za te usługi, zdaniem Komisji naraża prywatność użytkowników na nowe niebezpieczeństwa, czemu mają przeciwdziałać przepisy tej dyrektywy.

Na poziomie Unii Europejskiej początki regulacji dotyczących bezpieczeństwa w sektorze informatycznym zostały zawarte głównie w dyrektywie 2002/58/WE z 12 lipca 2002 r. o prywatności i łączności elektronicznej dotyczącej m.in. bezpieczeństwa publicznych sieci łączności elektronicznej[461], w decyzji ramowej 2005/222/WSiSW Rady z 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[462] oraz w rozporządzeniu (WE) 460/2004 z 10 marca 2004 r. ustanawiającym Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji[463]. Ponadto na szczególną uwagę w tym obszarze zasługują dwie dyrektywy: dyrektywa 2002/22/WE w sprawie usługi powszechnej[464] oraz dyrektywa 2002/20/WE w sprawie zezwoleń[465].

Zgodnie z dyrektywą 2002/58/WE państwa członkowskie powinny zapewnić, by sieci łączności elektronicznej mogły być wykorzystywane w celu przechowywania informacji na terminalu abonenta lub użytkownika tylko w przypadku zrozumiałego i wyczerpującego informowania użytkownika o celach przetwarzania oraz prawie sprzeciwu wobec niego. Tym samym zobowiązano dostawców publicznie dostępnych usług łączności elektronicznej do podjęcia właściwych środków technicznych i organizacyjnych w celu

zapewnienia bezpieczeństwa oferowanych przez siebie usług. Ponadto dyrektywa zobowiązuje państwa członkowskie do zapewnienia, za pomocą państwowego ustawodawstwa, poufności komunikacji i związanych z nią danych o ruchu za pośrednictwem dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej[466]. Należy zaznaczyć, że poufność nie ma zastosowania w przypadku przetwarzania danych na potrzeby udokumentowania transakcji lub prowadzenia korespondencji handlowej. Zgodnie z art. 5 ust. 3 dyrektywy 2002/58/WE dozwolone jest techniczne przechowywanie danych oraz dostęp do nich w celu wykonania lub ułatwiania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej lub w sytuacji, gdy jest to konieczne, aby dostarczyć usługi społeczeństwu informacyjnemu, wyraźnie zażądanej (zamawianej) przez abonenta lub użytkownika. Istotę tego przepisu stanowi generalna dopuszczalność wykorzystywania rozwiązań technologicznych dających usługodawcy dostęp do niektórych danych użytkowników końcowych[467].

Na mocy art. 13 omawianej dyrektywy zakazane jest dostarczanie niepożądanej poczty elektronicznej *(spamming)* oraz wykorzystywanie automatycznych systemów wywołujących, bez ingerencji człowieka, faksów lub poczty elektronicznej do celów marketingu bezpośredniego, chyba że wcześniej została uzyskana zgoda użytkownika na takie działania. Zakazano w szczególności wysyłania poczty elektronicznej do celów marketingu bezpośredniego, gdzie przerobiono lub ukryto tożsamość nadawcy, w którego imieniu wysyłano komunikat, lub bez aktualnego adresu, na który odbiorca może wysłać wniosek o zaprzestanie takich komunikatów[468].

W celu zapewnienia wysokiego i skutecznego poziomu bezpieczeństwa sieci i informacji we Wspólnocie oraz rozwijania kultury bezpieczeństwa sieci i informacji na rzecz obywateli, konsumentów, przedsiębiorstw oraz organizacji sektora publicznego Unii Europejskiej, a zatem zapewnienia płynnego funkcjonowania rynku wewnętrznego 10 marca 2004 r. ustanowiono Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji[469], będącą ośrodkiem

ekspertyzy ds. zagadnień związanych z bezpieczeństwem internetowym. Ma ona zapewniać pomoc władzom państw członkowskich, a w szczególności ich zespołom interwencyjnym w przypadku wystąpienia nadzwyczajnych sytuacji związanych z informatyką. Jej rolą jest przygotowywanie ekspertyz o wysokim poziomie szczegółowości i stosowanie ich do stymulowania szerokiej współpracy między instytucjami sektorów publicznego i prywatnego. Ponadto Agencja wspiera Komisję w technicznych pracach przygotowawczych dotyczących aktualizacji i rozwoju ustawodawstwa Wspólnoty w dziedzinie bezpieczeństwa sieci i informacji[470].

Do jej zadań należy także zbieranie stosownych informacji w celu przeanalizowania ryzyka bieżącego i powstającego (szczególnie w Europie), które może wpływać na dostępność i elastyczność sieci łączności elektronicznej oraz autentyczność, integralność i poufność informacji udostępnianych i przesyłanych przez sieci, a także dostarczanie wyników analiz państwom członkowskim i Komisji. Stwierdzono także, że Agencja powinna zajmować się doradztwem, oferować na żądanie pomoc w ramach swoich kompetencji, rozszerzać współpracę między różnymi instytucjami działającymi w obszarze bezpieczeństwa sieci i informacji, m.in. poprzez organizowanie regularnych konsultacji z przemysłem, uniwersytetami i innymi stosownymi sektorami oraz tworzenie sieci kontaktów dla organów Wspólnoty, organów sektora publicznego, wyznaczonych przez państwa członkowskie, sektora prywatnego oraz organów konsumenckich[471].

W dyrektywie o usłudze powszechnej zawarto regulacje dotyczące integralności sieci. Zgodnie z art. 23 tej dyrektywy państwa członkowskie są zobowiązane do podjęcia koniecznych środków w celu zapewnienia integralności stacjonarnej publicznej sieci telefonicznej oraz, w przypadku załamania sieci w wyniku katastrofy lub działania siły wyższej, dostępności usług stacjonarnej publicznej sieci telefonicznej i publicznie dostępnych usług telefonicznych. Podejmowane przez przedsiębiorstwa świadczące stacjonarne publicznie dostępne usługi telefoniczne w tym zakresie kroki

powinny mieścić się w granicach rozsądku w celu zapewnienia nieprzerwanego dostępu do służb ratunkowych. Dyrektywa o zezwoleniach określa natomiast zasady i warunki udzielania zezwoleń na udostępnienie sieci oraz świadczenie usług łączności elektronicznej. Wśród wymogów, jakie mogą być związane z uzyskaniem ogólnego zezwolenia, wymieniono obowiązki dotyczące zapewnienia bezpieczeństwa sieci i świadczonych usług: obowiązek utrzymania integralności sieci łączności powszechnej, w tym przez zapewnienie warunków mających zapobiegać zaburzeniom elektromagnetycznym między sieciami łączności elektronicznej lub usługami, oraz obowiązek zabezpieczenia sieci publicznej przed dostępem podmiotów nieuprawnionych.

Dyrektywa w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony została przyjęta 8 grudnia 2008 r.[472] W pierwszej części dyrektywy zawarto postanowienia dotyczące rozpoznania europejskiej infrastruktury krytycznej (EIK), które powinno odbywać się zgodnie z procedurą zaprezentowaną w załączniku do dyrektywy. Za przebieg procesu odpowiedzialne są państwa członkowskie. Wyróżniono dwa rodzaje kryteriów, które należy brać pod uwagę przy rozpoznawaniu infrastruktury na poziomie europejskim: kryteria przekrojowe mające zastosowanie do wszystkich sektorów oraz kryteria sektorowe charakterystyczne dla poszczególnych sektorów[473]. Kryteria przekrojowe to: kryterium ofiar w ludziach (oceniane w odniesieniu do ewentualnej liczby ofiar śmiertelnych lub liczby rannych), kryterium skutków ekonomicznych (oceniane w odniesieniu do wielkości strat ekonomicznych lub pogorszenia towarów bądź usług, w tym potencjalnych skutków ekologicznych) oraz kryterium skutków społecznych (oceniane w odniesieniu do wpływu na zaufanie opinii publicznej, cierpień fizycznych i zakłócenia codziennego życia, w tym utraty podstawowych usług). Ustalono dokładne progi mające zastosowanie do kryteriów przekrojowych. Kryteria te mają być niejawne, a stosowanie wytycznych – fakultatywne dla państw członkowskich. Rozpoznanie EIK ma obejmować sektory energetyczny i transportowy, w dalszej

kolejności może zostać zastosowane do rozpoznania kolejnych sektorów, przy czym priorytet nadano sektorowi technologii informacyjno-komunikacyjnych[474].

W art. 5 dyrektywy zobowiązano państwa członkowskie do opracowania bądź zweryfikowania Planu Ochrony Infrastruktury obejmującego składniki infrastruktury krytycznej należące do EIK oraz istniejące lub wdrażane rozwiązania służące ochronie tych składników. Przygotowując wspomniany plan, oprócz rozpoznania ważnych składników infrastruktury należy przeprowadzić co najmniej analizę ryzyka opartą na scenariuszach postępowania w przypadku zaistnienia poważnych zagrożeń, analizę słabych punktów każdego składnika infrastruktury oraz potencjalnych skutków, a także rozpoznać, wyznaczyć i ustalić hierarchię ważności środków ich ochrony[475]. Środki ochrony powinny obejmować m.in. stałe środki bezpieczeństwa, środki techniczne (w tym instalacje urządzeń wykrywających, kontrolę dostępu, środki zabezpieczające i zapobiegawcze), środki organizacyjne (w tym procedury sygnalizowania zagrożeń i zarządzania kryzysowego), środki kontrolno-weryfikacyjne, zasady komunikacji, podnoszenia świadomości, szkolenia z bezpieczeństwa systemów informacyjnych oraz doraźne środki ochrony uruchamiane w zależności od zmieniającego się poziomu ryzyka i zagrożenia. Ponadto w dyrektywie zobowiązano państwa członkowskie do utworzenia systemu zapewniającego właściwy i regularny nadzór nad planami bezpieczeństwa infrastruktury oraz sposobami ich wdrażania[476].

W ustawodawstwie Unii Europejskiej znajdują się również regulacje odnoszące się do kryminalizacji działań mających na celu rozpowszechnianie informacji zakazanych przez prawo, także za pośrednictwem sieci komputerowych. Dyrektywa nr 2011/93/UE z 13 grudnia 2011 r.[477] zawiera przepisy dotyczące zwalczania wykorzystywania seksualnego dzieci, w tym pornografii dziecięcej rozpowszechnianej za pośrednictwem Internetu. Ustanawia ona minimalne normy w sprawie określania przestępstw i kar dotyczących niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci, pornografii dziecięcej oraz

nagabywania dzieci dla celów seksualnych. Wprowadza również przepisy służące lepszemu zapobieganiu takim przestępstwom i lepszej ochronie pokrzywdzonych (art. 1). W art. 5 znalazły się postanowienia dotyczące przestępstw związanych z pornografią dziecięcą. Podobnie jak przepisy Dyrektywy Rady Europy z 2007 r. zalecają one kryminalizację określonych przestępstw, wskazując jednocześnie minimalne ustawowe sankcje za ich popełnienie. W art. 5 ust. 3 przewidziano kryminalizację świadomego uzyskiwania dostępu, za pośrednictwem technologii informacyjno-komunikacyjnych do pornografii dziecięcej, przy czym czyn ten powinien być opatrzony sankcją karną w maksymalnym wymiarze co najmniej roku pozbawienia wolności.

Z kolei dyrektywa 2013/40/UE[478] z 12 sierpnia 2013 r. zastąpiła dotyczącą tej samej problematyki wcześniejszą decyzję ramową Rady 2005/222/WSiSW[479] z 24 lutego 2005 r., stanowiąc jej rozwinięcie oraz uszczegółowienie. Celem dyrektywy jest usprawnienie współpracy właściwych organów państw członkowskich w dziedzinie ataków na systemy informatyczne oraz ustanowienie minimalnych norm dotyczących określania przestępstw i kar w dziedzinie ataków na systemy informatyczne.

Zgodnie z art. 2 ww. dyrektywy w sprawie ataków na systemy informatyczne *system informatyczny* oznacza wszelkie urządzenia lub grupę podłączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych komputerowych oraz danych przechowywanych, przetwarzanych, odzyskanych lub przekazanych przez nie w celach ich eksploatacji, użycia, ochrony lub utrzymania. *Dane komputerowe* oznaczają natomiast wszelkie przedstawienie faktów, informacji lub pojęć w formie odpowiedniej do przetwarzania w systemie informatycznym, włącznie z programem odpowiednim do spowodowania wykonania funkcji przez system. Terminem *bezprawne* określono dostęp lub ingerencję, na którą właściciel, inny posiadacz prawa do systemu lub jego części nie udzielił zgody lub która nie jest dozwolona na mocy prawa państwowego[480].

W celu zbliżenia porządków prawnych uznano, że w każdym państwie członkowskim nielegalny dostęp do systemu informatycznego oraz nielegalna ingerencja w system i dane powinny być karane jako przestępstwo. Nielegalny dostęp do systemu informatycznego rozumiany jest jako umyślny, bezprawny dostęp do całości lub części systemu informatycznego[481]. Państwa członkowskie mogą swobodnie zdecydować, czy jest on objęty oskarżeniem zawsze czy jedynie w sytuacji, gdy przestępstwo jest popełniane z naruszeniem zabezpieczenia. W myśl art. 4 dyrektywy nielegalną ingerencją w system jest bezprawne, umyślne, poważne naruszenie lub przerwanie funkcjonowania systemu informatycznego przez wprowadzanie, przekazywanie, uszkadzanie, usuwanie, niszczenie, zmienianie, zatajanie lub uczynienie niedostępnymi danych komputerowych. Nielegalna ingerencja w dane, zgodnie z art. 5 dyrektywy, oznacza umyślne i bezprawne usunięcie, uszkodzenie, pogorszenie, zmianę, zatajanie lub uczynienie niedostępnymi danych komputerowych w systemie informatycznym[482].

Zgodnie z art. 8 dyrektywy w sprawie ataków na systemy informatyczne karze podlegają również podżeganie do popełnienia wymienionych przestępstw, pomocnictwo w ich popełnieniu i usiłowanie ich popełnienia. Każde państwo członkowskie może zdecydować, czy usiłowanie uzyskania nielegalnego dostępu do systemu informatycznego będzie traktowane jak przestępstwo. Przestępstwa powinny podlegać karze co najmniej 2 lat pozbawienia wolności, kara ta ulega jednak zaostrzeniu, gdy przestępstwa nielegalnej ingerencji w system i dane oraz nielegalnego dostępu z naruszeniem zabezpieczeń zostały popełnione w ramach organizacji przestępczej lub spowodowały poważne szkody albo miały wpływ na istotne interesy. Podlegają one wówczas karze co najmniej 3 lat pozbawienia wolności. Stwierdzono, że do odpowiedzialności karnej może zostać pociągnięta nie tylko osoba fizyczna, lecz także osoba prawna[483].

W ustawodawstwie Unii Europejskiej znajdują się regulacje odnoszące się do kryminalizacji działań mających na celu

rozpowszechnianie informacji zakazanych przez prawo, także za pośrednictwem sieci komputerowych. Dyrektywa nr 2011/93/UE z 13 grudnia 2011 r.[484] zawiera przepisy dotyczące zwalczania wykorzystywania seksualnego dzieci, w tym pornografii dziecięcej rozpowszechnianej za pośrednictwem Internetu. Ustanawia ona minimalne normy odnoszące się do określania przestępstw i kar dotyczących niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci, pornografii dziecięcej oraz nagabywania dzieci dla celów seksualnych. Wprowadza ona również przepisy służące lepszemu zapobieganiu takim przestępstwom i lepszej ochronie pokrzywdzonych w ich wyniku (art. 1 dyrektywy). W art. 5 dyrektywy znalazły się postanowienia dotyczące przestępstw związanych z pornografią dziecięcą. Podobnie jak Dyrektywa Rady Europy z 2007 r. zalecają one kryminalizację określonych przestępstw, wskazując jednocześnie minimalne ustawowe sankcje za ich popełnienie. W art. 5 ust. 3 przewidziano kryminalizację świadomego uzyskiwania dostępu do pornografii dziecięcej za pośrednictwem technologii informacyjno-komunikacyjnych, przy czym czyn ten powinien być opatrzony sankcją karną w maksymalnym wymiarze co najmniej roku pozbawienia wolności.

Najnowszą agencją ustanowioną w celu zwalczania cyberprzestępczości jest Europejskie Centrum ds. Walki z Cyberprzestępczością. Zamiar jego ustanowienia Komisja ogłosiła w *Strategii bezpieczeństwa wewnętrznego UE w działaniu*[485], którą przyjęła 22 listopada 2010 r.[486] Uruchomiono je 11 stycznia 2013 r. Stanowi ono uzupełnienie wniosków ustawodawczych zawartych w dyrektywie dotyczącej ataków na systemy informatyczne oraz dyrektywie w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej. Centrum działa w ramach Europolu, z siedzibą w Hadze w Holandii. Do jego zadań należy przede wszystkim ochrona profili użytkowników serwisów społecznościowych przed zagrożeniami ze strony środowisk przestępczych oraz udzielanie pomocy w zwalczaniu przestępstw internetowych, które przynoszą poważne szkody.

Dyrektywa 2014/41/UE Parlamentu Europejskiego i Rady z 3 kwietnia 2014 r.[487] dotycząca europejskiego nakazu dochodzeniowego (END) w sprawach karnych w art. 1 ust. 1 definiuje szerszej pojęcia END niż to, które było zawarte w decyzji ramowej 2008/978/WSiSW[488]. W obecnym jej brzmieniu jest to orzeczenie sądowe wydane lub zatwierdzone przez organ wymiaru sprawiedliwości[489] państwa wydającego[490] w celu wezwania państwa wykonującego[491] do przeprowadzenia jednej lub kilku określonych czynności dochodzeniowych, aby uzyskać materiał dowodowy.

Dyrektywa obowiązuje od 21 maja 2014 r. Do 22 maja 2017 r. państwa członkowskie musiały wdrożyć niezbędne środki, by spełnić jej wymogi. Zastąpiła ona obowiązujące przepisy ratyfikowanej przez Polskę *Europejskiej konwencji o pomocy prawnej w sprawach karnych* z 1959 r. i *Konwencji o pomocy prawnej w sprawach karnych* między państwami członkowskimi UE z 2000 r., a także decyzji ramowej Rady 2003/577/WSiSW w sprawie wykonania w Unii Europejskiej postanowień o zabezpieczeniu mienia i środków dowodowych oraz decyzji ramowej 2008/978/WSiSW w sprawie europejskiego nakazu dowodowego.

Podobnie jak ENA europejski nakaz dowodowy (END) jest kolejnym instrumentem opierającym się na zasadzie wzajemnego uznawania, ułatwiającym w ten sposób współpracę między państwami członkowskimi UE, wyłączającym podwójne wymagania przestępczości na liście przestępstw, w tym terroryzmu. Procedura stosowania jest prosta, czynności są podejmowane bezpośrednio przez organy sądowe, jednak europejski nakaz dowodowy z 2008 r. jest często oceniany jako bezużyteczny, ponieważ wymaga pewności dotyczącej obecności dowodów w państwie wezwanym[492]. W związku z tym nowy instrument, jakim jest END, obejmuje prawie wszystkie czynności dochodzeniowe i nie ma tego wymogu. Instrumenty te mają kluczowe znaczenie w walce z wykorzystaniem Internetu do celów terrorystycznych, ponieważ umożliwiają one szybką współpracę międzynarodową.

END powinien umożliwić sądom, prokuratorom i innym organom dochodzeniowym bezpośrednie przekazywanie wniosków o

przeprowadzenie określonego dowodu, zabezpieczenie i przeszukanie mienia czy przesłuchanie w formie wideokonferencji. Organ sądowy kraju, do którego skierowano END, ma ograniczone przesłanki odmowy wykonania takiego wniosku (m.in. ze względu na kwestie bezpieczeństwa narodowego) oraz ściśle określone terminy jego realizacji. Co do zasady ma traktować europejskie nakazy tak samo jak te, które są wydawane przez organy krajowe.

Zgodnie z art. 3 zakresowi przedmiotowemu END podlega każda czynność dochodzeniowa poza utworzeniem wspólnego zespołu dochodzeniowo-śledczego oraz gromadzeniem materiału dowodowego w ramach takiego zespołu dochodzeniowo-śledczego, przewidzianego w art. 13 *Konwencji o pomocy w sprawach karnych między państwami członkowskimi Unii Europejskiej* oraz w decyzji ramowej Rady 2002/465/WSiSW, chyba że czynności te podejmowane są w celu zastosowania art.13 ust. 8 konwencji oraz art. 1 ust. 8 decyzji ramowej 2002/465/WSiSW[493].

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r.[494] w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, zwana dalej Dyrektywą NIS[495], ma na celu zapewnienie bezpieczeństwa informacji i stanowi wyzwanie dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa, a więc podmiotów gospodarczych świadczących usługi przy wykorzystaniu systemów teleinformatycznych, użytkowników cyberprzestrzeni, organów władzy publicznej, a także wyspecjalizowanych podmiotów zajmujących się bezpieczeństwem teleinformatycznym w sferze operacyjnej. Jest to tym bardziej istotne, że Polska jest ściśle powiązana z innymi państwami przez współpracę międzynarodową w ramach takich organizacji, jak UE, NATO, ONZ oraz OBWE. Współpraca ta odgrywa istotną rolę w walce z rosnącą liczbą incydentów powodowanych nielegalnymi działaniami w cyberprzestrzeni, prowadzącymi do strat materialnych i wizerunkowych. Dyrektywa formułuje obowiązki służące zapewnieniu cyberbezpieczeństwa systemom informacyjnym

w sektorach usług mających kluczowe znaczenie dla utrzymania krytycznej działalności społeczno-gospodarczej, a więc w energetyce, transporcie, bankowości, instytucjach finansowych, sektorze ochrony zdrowia, zaopatrzenia w wodę i infrastrukturze cyfrowej[496]. Wprowadza pojęcie operatora usługi kluczowej, czyli podmiotu świadczącego usługę kluczową z wykorzystaniem systemów informacyjnych, w przypadku której incydenty bezpieczeństwa teleinformatycznego mogłyby mieć istotny wpływ na jej świadczenie. Podjęcie prac związanych z kompleksowym uregulowaniem krajowego systemu cyberbezpieczeństwa wynika zatem z jednej strony z potrzeby zapewnienia systemowego podejścia do krajowego systemu cyberbezpieczeństwa w obliczu stale rosnących i dynamicznie zmieniających się zagrożeń cyberbezpieczeństwa dla funkcjonowania państwa, gospodarki i społeczeństwa, z drugiej – konieczności wdrożenia do polskiego porządku prawnego dyrektywy 2016/1148.

Dyrektywa 2016/1148 jest pierwszym aktem prawa UE w zakresie cyberbezpieczeństwa wprowadzającym regulacje międzysektorowe. Czas na implementację dyrektywy do porządków prawnych państw członkowskich upłynął 9 maja 2018 r. Tekst dyrektywy koncentruje się wokół trzech filarów:

- instytucji, które powinny powstać we wszystkich państwach członkowskich,
- współpracy na poziomie europejskim,
- zobowiązań w zakresie bezpieczeństwa sieci i informacji.

W zakresie filaru pierwszego każde państwo członkowskie jest zobligowane do ustanowienia organów właściwych ds. bezpieczeństwa sieci i informacji, odpowiedzialnych za monitorowanie stosowania jej przepisów w sektorach objętych jej zakresem. Ze względu na różnice w krajowych strukturach zarządzania państwa członkowskie mogą wyznaczać więcej niż jeden właściwy organ krajowy odpowiedzialny za wykonywanie zadań związanych z cyberbezpieczeństwem operatorów usług kluczowych i dostawców usług cyfrowych.

Ponadto w przypadku ustanowienia wielu organów właściwych każde państwo członkowskie musi ustanowić pojedynczy punkt kontaktowy (PPK), którego zadaniem jest wzmacnianie współpracy między państwami członkowskimi, gromadzenie informacji o incydentach w kraju i wzmacnianie wymiany informacji o znaczących, transnarodowych incydentach przez kontakt ze swoimi odpowiednikami z zagranicy[497].

Ostatnią wymaganą przez dyrektywę instytucją jest Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) obejmujący cały zakres podmiotowy regulacji. Państwa członkowskie mogą wskazać kilka CSIRT lub jeden, np. w obrębie organu właściwego. Dyrektywa zachowuje dużą elastyczność, jeżeli chodzi o wewnętrzne struktury systemu cyberbezpieczeństwa. Oznacza to, że kraje członkowskie mogą wyznaczyć jeden CSIRT narodowy dla całego kraju, kilka CSIRT poziomu narodowego bądź zbudować sieć CSIRT sektorowych.

Zakres podmiotowy dyrektywy ujęto w dwóch załącznikach. Załącznik II dotyczy operatorów usług kluczowych, załącznik III reguluje dostawców usług cyfrowych. Operatorów wskazanych w każdym z załączników obowiązują inne wymagania.

W przypadku dostawców usług cyfrowych (załącznik III) będzie obowiązywać bardziej łagodne i reaktywne podejście obejmujące działania nadzorcze *ex post*, tzn. po zaistnieniu incydentu, i tylko przez to państwo, na którego terenie dostawca usługi ma swoją siedzibę. Podmioty z załącznika III nie będą podlegały opisanemu wcześniej procesowi identyfikacji i raportowania, jak w przypadku operatorów usług kluczowych. Takie podejście spowodowane jest międzynarodowym działaniem operatorów dostarczających usługi cyfrowe, a tym samym obawą przed fragmentaryzacją jednolitego rynku cyfrowego UE. W wyniku negocjacji ustalono, że regulacjami zostaną objęte serwisy zakupowe, wyszukiwarki internetowe oraz usługi chmury obliczeniowej.

Dyrektywa nie dotyczy bezpośrednio usług administracji publicznej, o ile nie są to usługi kluczowe wymienione w niej. Najważniejsze jest jednak to, że dyrektywa 2016/1148 stanowi

harmonizację minimalną i nie ogranicza możliwości państw członkowskich do regulowania problematyki bezpieczeństwa teleinformatycznego administracji publicznej, a także objęcia zakresem większej liczby podmiotów. To należy do państw członkowskich.

Specyfika uregulowania dostawców usług cyfrowych polega na tym, że zainteresowany właściwy organ powinien podejmować działania wyłącznie wtedy, gdy otrzymał dowód, np. od dostawcy usług cyfrowych, innego właściwego organu, w tym właściwego organu innego państwa członkowskiego lub od użytkownika usługi, że dostawca usług cyfrowych nie spełnia wymogów niniejszej dyrektywy, w szczególności w wyniku wystąpienia incydentu. Właściwy organ nie powinien mieć ogólnego obowiązku nadzorowania dostawców usług cyfrowych.

Drugi filar dyrektywy obejmuje współpracę między państwami członkowskimi. Dyrektywa 2016/1148 wprowadza mechanizmy współpracy na dwóch poziomach: technicznym i polityczno-strategicznym. Współpraca techniczna ma być zapewniona przez europejską sieć CISRT oraz stworzenie mechanizmów wymiany informacji o incydentach transgranicznych między CSIRT wyznaczonymi dla operatorów usług kluczowych a dostawcami usług cyfrowych. Z kolei współpraca na poziomie polityczno-strategicznym ma być realizowana przez utworzenie Grupy Współpracy, która zajmie się wypracowaniem wspólnych koncepcji strategicznych oraz będzie przyjmowała m.in. roczne raporty od właściwych organów.

Trzecim filarem dyrektywy są zobowiązania w zakresie bezpieczeństwa sieci i informacji, które są różne w zależności od załącznika. Operatorzy usług kluczowych zostaną zobowiązani do dokonania oceny zagrożeń cyberbezpieczeństwa, na jakie są narażeni, oraz do przyjęcia odpowiednich i proporcjonalnych środków mających na celu zapewnienie bezpieczeństwa sieci i informacji. Podmioty te mają zgłaszać właściwym organom wszelkie incydenty poważnie zagrażające ich sieciom i systemom informatycznym, mogące znacząco zakłócić ciągłość działania kluczowych usług (raportowanie obowiązkowe). Raportowaniu będą

podlegać incydenty o „znaczącym wpływie na ciągłość działania operatorów", co *de facto* oznacza, że progi raportowania określą państwa członkowskie w procesie implementacji. Podmioty załącznika III zostaną natomiast objęte regulacją reaktywnym nadzorem *ex post*.

Dyrektywa nakłada także na państwa członkowskie obowiązek przyjęcia narodowej strategii bezpieczeństwa sieci i informacji, w której zostaną określone m.in. narodowe cele i priorytety w dziedzinie cyberbezpieczeństwa, role i obowiązki organów administracji publicznej w procesie osiągania wyznaczonych celów, zasady współpracy sektora publicznego i prywatnego oraz krajowa analiza ryzyka i zadania w zakresie edukacji na rzecz cyberbezpieczeństwa. Przepisy dyrektywy umożliwiają stworzenie zarówno scentralizowanego systemu na poziomie krajowym, jak i podzielenie kompetencji między różne podmioty wymieniające informacje za pomocą opracowanych mechanizmów współpracy. Ponadto dyrektywa zobowiązuje wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu krajowych zdolności w dziedzinie bezpieczeństwa teleinformatycznego i daje organom publicznym konkretne narzędzie do przeciwdziałania incydentom w cyberprzestrzeni oraz reakcji na nie. Będzie to możliwe m.in. dzięki nałożonym obowiązkom raportowania i przygotowania krajowych strategii, skoordynowaniu przepływu informacji oraz zinstytucjonalizowaniu współpracy CSIRT[498].

W przypadku rozporządzenia GDRP należy zacząć od wskazania, że to nie Unia Europejska, lecz Rada Europy była organizacją, w której ramach po raz pierwszy wypracowano podstawowy standard ochrony danych osobowych. W tym kontekście należy wspomnieć o *Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych*, sporządzonej w Strasburgu 28 stycznia1981 r.[499], która wraz z protokołem dodatkowym do konwencji oraz protokołem nr 223 modernizującym konwencję z 10 października 2018 r. reguluje podstawy systemu ochrony danych osobowych i ma zastosowanie również do tej

szczególnej dziedziny, jaką jest przetwarzanie danych osobowych przez organy ścigania i organy wymiaru sprawiedliwości.

Na mocy art. 3 ust. 1 konwencji nr 108 strony zobowiązały się stosować ją zarówno do zautomatyzowanych zbiorów danych osobowych, jak i automatycznego przetwarzania danych osobowych w sektorach publicznym i prywatnym. W związku z tym konwencja nr 108 ma zastosowanie do ochrony danych osobowych osób będących uczestnikami postępowań sądowych i karnych wszczynanych przez organy ścigania, przetwarzanych automatycznie, jeżeli państwo nie wyłączyło tych kategorii na podstawie odrębnie złożonej deklaracji. Państwa mogły tak uczynić na podstawie art. 3 ust. 2 lit. a ww. konwencji, który stanowi, że każde państwo przy podpisywaniu konwencji lub składaniu dokumentów ratyfikacyjnych, przyjęciu, potwierdzeniu lub przystąpieniu albo w każdym późniejszym terminie może złożyć na ręce Sekretarza Generalnego Rady Europy deklarację, że nie będzie stosować niniejszej konwencji do niektórych kategorii zautomatyzowanych zbiorów danych osobowych, których lista zostanie przedłożona.

Konwencję nr 108 należy traktować raczej jako akt o charakterze wyznaczającym standard podstawowy niż mający zastosowanie praktyczne. Państwa członkowskie stopniowo podejmują też decyzje o podpisaniu wspomnianego protokołu nr 223 z 10 października 2018 r., który ma na celu modernizację konwencji nr 108.

Do czasu wejścia w życie Traktatu z Lizbony możliwości prawne podjęcia się przez instytucje WE uregulowania zasad przetwarzania danych osobowych w obszarze współpracy policyjnej i sądowej w sprawach karnych były bardzo ograniczone. Wiązało się to z dotychczasową tzw. filarową strukturą UE oraz odmiennościami systemu prawnego w obszarze współpracy gospodarczej. Rozwój systemu ochrony danych osobowych, podobnie jak rozwój współpracy państw członkowskich w innych dziedzinach nie był zatem równomierny. Przetwarzanie danych osobowych zostało objęte spójnymi regulacjami w obszarze podlegającym zasadom I filara UE, wynikającymi przede wszystkim z dyrektywy ogólnej w sprawie ochrony danych (dyrektywa 95/46/WE). Od daty jej przyjęcia

w ramach I filaru UE ukształtowało się *acquis communautaire* regulujące problematykę ochrony danych, a w szczególnych obszarach, np. dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady, zostało też wypracowane orzecznictwo Trybunału Sprawiedliwości. W przypadku dawnego III filaru UE rozwój prawodawstwa następował w odwrotnej kolejności – rozwijało się ono *ad hoc*, w zależności od potrzeb, w związku z powoływaniem kolejnych agend UE bądź kolejnych systemów wymiany informacji. Dopiero w 2008 r. przyjęto decyzję ramową Rady 2008/977/WSiSW z 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych[500]. Akt ten miał charakter ogólny w tym znaczeniu, że nie dotyczył ani szczególnego systemu, ani formy przetwarzania. Nie miał również charakteru powszechnego, regulował bowiem wyłącznie zasady przetwarzania danych osobowych w relacjach transgranicznych między państwami członkowskimi (chociaż pierwotne zamierzenia były inne). Dotychczasowe regulacje sektorowe również przestały wystarczać, rozwiązania krajowe okazały się rozbieżne i pojawiła się potrzeba zintegrowania całości rozproszonych rozwiązań.

Po kilku latach od wejścia w życie decyzji ramowej 2008/977/WSiSW na forum UE, również w związku z pojawieniem się nowych podstaw traktatowych (art. 16 TFUE), zaczęto zastanawiać się nad podjęciem tematu reformy obowiązujących rozwiązań. Jako istotne przyczyny zajęcia się tą kwestią wskazano m.in. ograniczony zakres przedmiotowy decyzji ramowej. Poza zakresem regulacji było przetwarzanie danych wewnątrz państw członkowskich, które nadal mogły te kwestie regulować w sposób dowolny, zgodny jedynie z ogólnymi wskazówkami wynikającymi z konwencji nr 108. Problem braku spójności rozwiązań w poszczególnych państwach członkowskich był szczególnie widoczny w tych przypadkach, w których sprawy krajowe były często prowadzone na podstawie danych pochodzących z różnych źródeł. W momencie zbierania danych przez organy właściwe nie wiadomo, czy na późniejszym etapie nie zostaną one wykorzystane w kontekście transgranicznym.

Od wejścia w życie Traktatu z Lizbony możliwe stało się zatem podjęcie dyskusji na temat reformy systemu ochrony danych w ramach współpracy policyjnej i sądowej w sprawach karnych, ponieważ pojawiły się nowe ramy traktatowe, w szczególności art. 16 TFUE i art. 8 KPP, stanowiące podstawę prawną przyjmowania norm dotyczących ochrony danych również w obszarze współpracy policyjnej i sądowej w sprawach karnych. Tym samym Komisja mogła przedstawić projekt dyrektywy[501] regulujący tę materię w założeniu w sposób kompleksowy, mający na celu zapewnienie jednolitego poziomu ochrony, przy jednoczesnym poszanowaniu specyfiki omawianego obszaru. Prace nad uchwaleniem dyrektywy 2016/680 trwały ponad cztery lata. Jako przyczyny podjęcia reformy systemu ochrony danych wskazywano przede wszystkim zmiany technologiczne, wzrost znaczenia globalnej wymiany danych oraz luki w systemie ochrony rynku wewnętrznego. Jak już wspomniano, Komisja wybrała instrument dyrektywy w celu uregulowania kwestii przetwarzania danych osobowych w obszarze współpracy policyjnej i sądowej w sprawach karnych.

Dyrektywa 2016/680 została uchwalona – podobnie jak RODO – 27 kwietnia 2016 r. (weszła w życie 5 maja 2016 r.), wyznaczając termin implementacji dla państw członkowskich na 6 maja 2018 r. W drodze wyjątku dopuszczono pewne odstępstwa od tego terminu, związane z koniecznością dostosowania już istniejących zautomatyzowanych systemów przetwarzania danych[502].

Dyrektywa 2016/680 została przyjęta w celach określonych w jej art. 1[503]. Podobnie jak w przypadku RODO są to w istocie dwa odrębne cele. Po pierwsze, państwa członkowskie zostały zobowiązane do ochrony praw podstawowych i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych, po drugie, do zapewnienia, by wymiana danych osobowych przez właściwe organy w Unii, jeżeli wynika z prawa Unii lub prawa krajowego, nie była ograniczana ani zakazywana z powodów dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Cele te zostały zapisane w art. 1 ust. 2 dyrektywy 2016/680 jako równoprawne, chociaż mogą

wydawać się niespójne. Zadaniem prawodawcy krajowego, który implementował postanowienia dyrektywy 2016/680, jest zapewnienie, by została zachowana należyta równowaga między tymi celami. Prawodawca unijny zapewnił ku temu możliwości, zostawiając szeroki margines swobody w wielu przepisach dyrektywy (w przeciwieństwie do RODO).

Wydaje się, że prawodawca unijny na pierwszym miejscu stawia ochronę praw podstawowych jednostki, na co wskazuje treść art. 1 ust. 3 dyrektywy 2016/680, dopuszczającą ustanowienie przez państwa członkowskie zabezpieczeń wyższych niż zabezpieczenia przewidziane w dyrektywie dla ochrony praw i wolności osoby, której dane dotyczą, w związku z przetwarzaniem danych osobowych przez właściwe organy. Bez wątpienia jednak nie jest tak, by państwa członkowskie mogły – na podstawie przepisów dyrektywy – zrealizować wyłącznie jeden cel, pomijając cel drugi, np. gwarantując właściwym organom szerokie możliwości przetwarzania danych osobowych, nie zapewniając gwarancji ich ochrony. Należy podkreślić, że cele dyrektywy i ich określenie są istotne dla organów krajowych stosujących przepisy wdrażające dyrektywę. Interpretacja przepisów krajowych musi bowiem uwzględniać cel aktu wdrażanego – wykładnia celowościowa jest podstawową, jaka powinna być stosowana w przypadku aktów prawa UE.

Trzeba również pamiętać, że w założeniu zakres stosowania RODO i dyrektywy 2016/680 jest rozłączny. W art. 2 ust. 2 lit. c RODO wskazano wyraźnie, że nie ma ono zastosowania do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. To jest właśnie zakres dyrektywy 2016/680, ale warto przypomnieć, że w motywie 11 preambuły dyrektywy 2016/680 wskazano wyraźnie, że RODO ma zastosowanie wtedy, gdy organ lub podmiot zbiera dane osobowe do innych celów, a następnie dane te przetwarza w celu realizacji obowiązku prawnego, któremu podlega. Jako przykład podano przypadek, w którym określone instytucje finansowe zatrzymują przetwarzane

dane do celów postępowania przygotowawczego, wykrywania lub ścigania czynów zabronionych i udostępniają takie dane osobowe tylko właściwym organom krajowym w konkretnych sytuacjach i w zgodzie z prawem państwa członkowskiego. Możliwa jest również sytuacja, kiedy organy, do których obowiązków należy w pierwszej kolejności zapobieganie i zwalczanie przestępczości, mają również inne zadania. W takim przypadku do zadań, które nie wchodzą w zakres dyrektywy 2016/680, są stosowane przepisy RODO[504].

Trzeba też pamiętać, że ani RODO, ani dyrektywa 2016/680 nie mają zastosowania do przetwarzania danych osobowych w toku działalności wykraczającej poza zakres prawa Unii. Zarówno w preambule do RODO (motyw 16), jak i dyrektywy 2016/680 (motyw 14) jako przykład podaje się czynności dotyczące bezpieczeństwa narodowego, ale nie jest to jedyna możliwość. O ile na gruncie RODO problem ten ma istotne znaczenie, a wyznaczenie zakresu stosowania prawa UE jest ważne, by w ogóle stwierdzić, czy RODO w danym przypadku ma zastosowanie, o tyle na gruncie ODPU, czyli ustawy wdrażającej dyrektywę 2016/680, sprawa jest mniej istotna z tego względu, że ustawodawca krajowy miał możliwość wyjść poza to ograniczenie i poddać całościowej regulacji wszystkie sytuacje związane z przetwarzaniem danych osobowych do celów określonych w art. 1 ODPU. Nawet jeśli stwierdzono by, że do konkretnej sytuacji dyrektywa 2016/680 nie miałaby zastosowania ze względu na to, że sprawa znajduje się „poza zakresem prawa UE", nie ma jednak przeszkód, by wchodziła ona w zakres zastosowania ODPU, jeśli ustawodawca krajowy tak zdecydował[505].

4.2.3. INSTYTUCJONALNY WYMIAR ZWALCZANIA CYBERPRZESTĘPCZOŚCI W PRAWIE UNII EUROPEJSKIEJ

Jak wspomniano, 10 marca 2004 r. ustanowiono Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji[506], aby zapewnić wysoki i skuteczny poziom bezpieczeństwa sieci i informacji w Unii Europejskiej oraz rozwijać kultury bezpieczeństwa sieci i informacji na rzecz obywateli, konsumentów, przedsiębiorstw oraz organizacji

sektora publicznego Unii Europejskiej, czyli zapewnienia płynnego funkcjonowania rynku wewnętrznego. Agencja jest ośrodkiem ekspertyzy ds. zagadnień związanych z bezpieczeństwem internetowym, a jej celem jest zapewnienie pomocy władzom państw członkowskich, w szczególności ich zespołom interwencyjnym, w przypadku nadzwyczajnych sytuacji związanych z informatyką. Opracowuje ekspertyzy o wysokim poziomie szczegółowości, które można stosować do podejmowania współpracy między instytucjami sektorów publicznego i prywatnego. Ponadto wspiera Komisję w technicznych pracach przygotowawczych nad aktualizacją i rozwojem ustawodawstwa Wspólnoty w sprawach bezpieczeństwa sieci i informacji[507].

W rozporządzeniu ustanawiającym Agencję zapisano, że powinna ona wykonywać swoje zadania, współpracując ściśle z państwami członkowskimi, powinna być też otwarta na kontakty ze wspólnotą biznesową, przemysłem i innymi właściwymi udziałowcami. Ponieważ sieci elektroniczne stanowią w dużym stopniu własność prywatną, Agencja powinna opierać się na danych wejściowych pochodzących z sektora prywatnego oraz na współpracy z nim. Do obowiązków Agencji, poza opisanymi na s. 44, należy:

- ułatwianie współpracy Komisji z państwami członkowskimi w zakresie dotyczącym bezpieczeństwa sieci i informacji,
- przyczynianie się do wzrostu świadomości i dostępności aktualnych informacji na temat bezpieczeństwa sieci i informacji w sektorach publicznym i prywatnym,
- wspieranie Komisji i państw członkowskich w dialogu dotyczącym bezpieczeństwa sprzętu i oprogramowania,
- śledzenie rozwoju norm w tym zakresie,
- skuteczne stosowanie technologii zapobiegających powstawaniu ryzyka,
- współpraca z państwami trzecimi i organizacjami międzynarodowymi w celu promocji bezpieczeństwa sieci i informacji,
- wyrażanie własnych niezależnych opinii.

Strukturę Agencji tworzą Zarząd, dyrektor naczelny, który nią zarządza, oraz Stała Grupa Udziałowców składająca się z ekspertów reprezentujących przemysł technologii informacyjnych i łączności, grupy konsumenckie oraz ekspertów akademickich z zakresu bezpieczeństwa sieci i informacji. W skład Zarządu wchodzi jeden przedstawiciel każdego z państw członkowskich, trzech przedstawicieli wyznaczonych przez Komisję oraz trzech przedstawicieli bez prawa głosowania, zaproponowanych przez Komisję i wyznaczonych przez Radę. Zarząd określa ogólną orientację działania Agencji i zapewnia funkcjonowanie Agencji zgodnie z zasadami określonymi w rozporządzeniu. Gwarantuje również spójność pracy Agencji z działaniami państw członkowskich i Wspólnoty.

Należy wspomnieć o zaangażowaniu Unii Europejskiej w zwalczanie spamu. Stwierdzono, że aby skutecznie walczyć z rozprzestrzeniającym się spamem, należy podjąć działania na poziomie ponadnarodowym. W tym celu z inicjatywy Komisji Europejskiej została utworzona nieformalna grupa Contact Network of Spam Enforcement Authorities (CNSA) składająca się z przedstawicieli państw członkowskich Unii Europejskiej zaangażowanych w walkę ze spamem. Zadaniem CNSA jest wymiana informacji lub skarg między organizacjami narodowymi, wspólne ściganie przestępstw oraz wypracowywanie nie *best practice* (najlepszych praktyk) w zakresie zwalczania przesyłanej na dużą skalę niezamówionej informacji handlowej, naruszającej postanowienia art. 13 dyrektywy 2002/58/WE o prywatności i łączności elektronicznej[97].

Kolejną agencją ustanowioną w celu zwalczania cyberprzestępczości, o czym wcześniej wspomniano, jest Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3), którego głównym celem działania jest walka z cyberprzestępstwami w różnej postaci.

Aby zrealizować wymienione cele, EC3:

- jest centralnym ośrodkiem wymiany informacji karnych i wywiadowczych,

- wspiera państwa członkowskie w przeprowadzaniu operacji dochodzeniowo-śledczych,
- przeprowadza szkolenia,
- zapewnia wysoko wyspecjalizowanych specjalistów i ekspertyzy kryminalistyczne.

European Cybercrime Centre (EC3) zostało podzielone na kilka punktów kontaktowych (*focal points* – FP) zajmujących się określonymi obszarami działania. FP Terminal zapewnia wsparcie organów ścigania w sprawach dotyczących oszustw płatniczych, m.in. we współpracy z sektorem prywatnym i innymi organami, np. Europejskim Bankiem Centralnym i bankami krajowymi. Ponadto dąży do zapewnienia bezpieczeństwa i zaufania klientów w elektronicznych i internetowych transakcjach płatniczych oraz w transakcjach zawieranych przy użyciu kart płatniczych. Jednostka tworzy raporty analityczne dostarczające dane dotyczące np. rachunków bankowych, adresów e-mail oraz numerów telefonów. FP Cyborg wspiera państwa członkowskie UE w zakresie zapobiegania różnym formom cyberprzestępczości wpływającym na systemy sieciowej infrastruktury krytycznej i zwalczania ich. Szczególny nacisk położono na działania zorganizowanych grup przestępczych generujących duże zyski. Pracuje nad szeroką gamą zaawansowanych technologicznie przestępstw takich, jak haking, phishing, kradzież tożsamości, *malware*. FP Cyborg zapewnia analizę operacyjną i kryminalistyczną, wsparcie techniczne oraz badania cyfrowe dla państw członkowskich zarówno na miejscu (np. obecność ekspertów w trakcie przeszukań), jak i bezpośrednio z centrali Europolu. Powołany w celu walki z seksualnym wykorzystywaniem dzieci FP Twins zapewnia pomoc w zwalczaniu rozpowszechniania materiałów pedofilskich w Internecie, identyfikacji ofiar i przestępców, cyfrowego śledzenia sprawców, przechwytywaniu przesyłanych i informacji.

W ramach EC3 1 sierpnia 2014 r. powołano wspólną grupę zadaniową ds. cyberprzestępczości (EU Joint Cybercrime Action Taskforce – J-CAT). W jej skład weszli specjaliści z Austrii, Francji, Hiszpanii, Holandii, Niemiec, Włoch, Wielkiej Brytanii oraz Kanady, i

Stanów Zjednoczonych[508]. Na chwilę obecną dołączyła również Australia, Kolumbia, Polska, Szwecja, Rumunia i Szwajcaria. Współpraca tej grupy polega na wzajemnym przekazywaniu informacji wywiadowczych, które są pomocne w ustalaniu zadań, priorytetów w walce z cyberprzestępczością i zwalczaniu jej. W skład J-CAT wchodzą oficerowie łącznikowi posiadający specjalistyczne wyszkolenie w dziedzinie cyberprzestępczości i cyberbezpieczeństwa. Pochodzą z krajów Unii Europejskiej, organów ścigania spoza UE (m.in. USA reprezentowanych przez trzy agencje: FBI, Secret Service oraz Urząd Imigracyjny i Celny) oraz EC3.

Zadaniem J-CAT jest aktywne prowadzenie wywiadu, zbieranie informacji i przeprowadzanie skoordynowanych działań przeciwko cyberprzestępczości. Osiągnięcie tego celu ma nastąpić przez koordynację działań, wspólne ustalanie priorytetów, przygotowanie, wszczynanie i prowadzenie dochodzeń transgranicznych. J-CAT zajmuje się cyberprzestępstwami takimi, jak malware, botnety, oszustwa online (systemy płatności online, stosowanie inżynierii społecznej), pranie pieniędzy, w tym walut wirtualnych, oraz nadużyciami seksualnymi dzieci w cyberprzestrzeni.

Instytucją zwalczającą terroryzm i cyberterroryzm w UE jest Europol (Agencja Unii Europejskiej ds. Współpracy Organów Ścigania) odpowiedzialny za wywiad kryminalny. Jest on najważniejszą instytucją UE w tym obszarze. W roku 1999 zakres jego kompetencji został rozszerzony do walki z międzynarodowym terroryzmem. Wcześniej do jego zadań należało gromadzenie, przekazywanie i analiza danych dostarczonych przez państwowe organy policyjne oraz państwowe jednostki kontaktowe. Europol nie korzystał z żadnych uprawnień operacyjnych i nawet dostarczanie danych z państwowych źródeł różniło się w zależności od państwa członkowskiego. To jedyna stała centralna struktura policji UE. Konwencja o utworzeniu Europolu została podpisana 26 lipca 1995 r. w Brukseli, a biuro zaczęło formalnie działać w połowie 1999 r. W art. 2 ust.1 konwencji zapisano, że jednym z jej głównych celów jest udoskonalenie i wzmocnienie efektywności działania oraz wsparcie

instytucji odpowiedzialnych w Unii Europejskiej za zapobieganie terroryzmowi i cyberterroryzmowi oraz walkę z tymi zagrożeniami.

Zadaniem Europolu stało się zwalczanie oraz wykrywanie przestępstw przeciwko życiu, zdrowiu, wolności osobistej lub majątkowi, które zostały lub mogą zostać popełnione w trakcie działań terrorystycznych. Zgodnie z brzmieniem konwencji Europol miał się zajmować przestępstwami terrorystycznymi dopiero po dwóch latach od ratyfikacji umowy. Decyzję w tej sprawie podjęto w grudniu 1998 r. W ramach Europolu następuje wymiana informacji z państwami członkowskimi. Opracowano także bazę danych zawierającą listę środków prawnych i instytucjonalnych państw członkowskich oraz ich kompetencji dotyczących walki z terroryzmem. Jakość tej współpracy pozostawia jednak wiele do życzenia, gdyż państwa członkowskie nie były do tej pory chętne do zbyt otwartej wymiany informacji zgodnie z postanowieniami *Wspólnego działania* z 1996 r. Dokument ten dotyczy stworzenia i prowadzenia wszechstronnego zbioru danych w dziedzinie walki z terroryzmem w celu ułatwienia współpracy w zwalczaniu wszelkich postaci terroryzmu między państwami Unii[509].

Na podstawie art. 88 ust. 1 TFUE zadaniem[510] Europolu stało się wspieranie i wzmacnianie działań organów policyjnych i innych organów ścigania państw unijnych, a także ich wzajemnej współpracy w zapobieganiu i zwalczaniu poważnej przestępczości dotykającej dwóch lub więcej państw, terroryzmu oraz form przestępczości naruszających wspólny interes objęty polityką UE. Wszelkie działania operacyjne Europolu są prowadzone w powiązaniu i w porozumieniu z organami państwa członkowskiego, którego terytorium dotyczą. Stosowanie środków przymusu należy do wyłącznej kompetencji właściwych organów państwowych.

Europol zatrudnia przedstawicieli państwowych organów ścigania (policji, służb celnych, imigracyjnych itp.). W skład jego zarządu wchodzą po jednym przedstawicielu każdego państwa UE. Do zadań Europolu należy zapewnienie ścisłej i bardziej efektywnej współpracy w zakresie zapobiegania i zwalczania międzynarodowej przestępczości zorganizowanej, w szczególności:

- handlu narkotykami,
- sieci przemytu nielegalnych imigrantów,
- nielegalnego handlu pojazdami,
- handlu ludźmi, w tym pornografii dziecięcej,
- fałszowania pieniędzy i innych środków płatniczych,
- handlu substancjami radioaktywnymi i materiałami jądrowymi,
- terroryzmu i cyberterroryzmu[511].

Ponadto Europol jest odpowiedzialny za wdrożenie i prowadzenie systemu komputerowego umożliwiającego wprowadzanie, udostępnianie i analizę odpowiednich danych. Wspólny organ nadzorczy, w którego skład wchodzi dwóch ekspertów ds. ochrony danych, zapewnia właściwe wykorzystywanie wszelkich danych osobowych będących w posiadaniu Europolu. Europol podlega Radzie ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych, czyli ministrom sprawiedliwości i spraw wewnętrznych wszystkich państw UE[512].

Na bazie tych doświadczeń powołano System Informacyjny Schengen (SIS), który ułatwiał przekraczanie granic obywatelom UE, prowadząc jednocześnie kontrolę i ewidencję osób z państw trzecich[513]. Obok poprawy kontroli na zewnętrznych granicach państw przewidywano przede wszystkim poprawę współpracy policji i wymiany informacji, co powinno zapobiegać sytuacji, w której przestępcy bez przeszkód działaliby ponad granicami prawa. Wdrożenie środków uzupełniających natrafiło na spore trudności. Między państwami układu istniały różne zapatrywania na prawo posiadania broni i politykę dotyczącą narkotyków, dlatego Układ Wykonawczy do układu z Schengen (tzw. Schengen II) mógł zostać podpisany dopiero 19 czerwca 1990 r.[514] Przewidywał on m.in. utworzenie SIS. Konieczne było również uzgodnienie szeroko zakrojonych działań dotyczących ochrony danych. Obecnie funkcjonuje System Informacyjny Schengen drugiej generacji[515], tzw. SIS II[516].

Europol podjął wiele działań dotyczących walki z cyberprzestępczością i nielegalnymi działaniami w przestrzeni

wirtualnej. Kluczowym zagadnieniem jest prewencja i wymiana informacji, doświadczeń, metod działania oraz międzynarodowa współpraca między poszczególnymi państwami. W tym celu Europol systematycznie organizuje szkolenia poruszające najważniejsze problemy związane ze zwalczaniem cyberprzestępczości.

W dokumencie *Cybercrime: improving international cooperation*[517] Europol przedstawił czynniki, które uznał za istotne z punktu widzenia transgranicznego, międzynarodowego zwalczania przestępczości zorganizowanej, cyberprzestępczości i terroryzmu. Wskazał, że podstawą do transgranicznej pomocy prawnej jest wiele konwencji i porozumień, wśród których, w odniesieniu do cyberprzestępczości, najbardziej istotna jest *Konwencja o cyberprzestępczości* z 2001 r. Dla współpracy transgranicznej najbardziej korzystne jest wzajemne uznawanie procedury karnej, szczególnie metod pozyskiwania i zabezpieczenia dowodów w taki sposób, by dowody zebrane zgodnie z prawem w jednym państwie mogły posłużyć za dowód popełnienia przestępstwa w innym państwie.

Z punktu widzenia walki z cyberprzestępczością szczególnie istotne jest szkolenie społeczeństwa i organów ścigania. Szybki rozwój technologii powoduje, że szkolenia powinny mieć charakter ciągły, zwłaszcza w zakresie nowych technik kryminalistyki cyfrowej. Konieczne jest stałe aktualizowanie materiałów szkoleniowych, wymiana informacji i najlepszych praktyk. Eksperci Europolu słusznie akcentują, że znaczące w skutecznej walce z cyberprzestępczością jest posiadanie odpowiednich narzędzi do przetwarzania dużych ilości danych[518].

Kolejną instytucją działającą w tym obszarze jest Eurojust, który wzmocnił współpracę między organami ścigania państw członkowskich i osiągnął znaczący sukces operacyjny. Transpozycja decyzji nr 2002/187/WSiSW[519] balansuje na pograniczu sukcesu. Dla większej efektywności władze państw członkowskich i Kolegium powinny podjąć działania mające na celu wyjaśnienie i wzmocnienie ich uprawnień, a także określenie podstawy wspólnych minimalnych kompetencji. Brak spójnych uprawnień państwowych członków

utrudnia nawiązanie w pełni skutecznej współpracy. Decyzje wyznaczające i opisujące zakres obowiązków i status państwowych użytkowników nie nadają im realnej władzy, dlatego zgodnie z art. 1 decyzji ramowej Rady z 13 czerwca 2002 r. w sprawie wspólnych zespołów dochodzeniowo-śledczych, dwa lub więcej państw członkowskich UE w drodze wzajemnych umów mogą tworzyć wspólne zespoły dochodzeniowo-śledcze w szczególnym celu[520] i na określony czas, z możliwością przedłużenia ich działalności na podstawie wzajemnej zgody w celu prowadzenia śledztw w sprawach karnych w jednym lub więcej państwie członkowskim współtworzącym zespół. Skład zespołu zostaje potwierdzony w umowie. Z wnioskiem o utworzenie wspólnego zespołu dochodzeniowo-śledczego może wystąpić każde z zainteresowanych państw członkowskich. Zespół powstaje w tym z państw członkowskich, w którym przewiduje się prowadzenie śledztwa. Państwa członkowskie ustalają także wykorzystanie kompetencji ich organów na swoim terytorium.

W celu zwiększenia operacyjnej współpracy w ramach Eurojustu państwa członkowskie są zobowiązane przekazywać informacje na swój temat do jednostki oraz wzmacniać organy państwowe. Korzystają również z usług ekspertów państwowych. Organami wewnętrznymi Eurojustu są: Kolegium[521], dyrektor administracyjny[522], funkcjonariusz ds. ochrony danych[523].

Eurojust może działać poprzez swoich przedstawicieli państwowych i jako Kolegium. Występując przez swoich przedstawicieli państwowych, może podjąć postępowanie na poziomie europejskim, ułatwiać współpracę władzom państw członkowskich, wspomagać dochodzenie w państwie członkowskim i zaproponować ściganie, przekazywać wnioski o pomoc sądową, współpracować z EJN. Jako Kolegium może natomiast odgrywać pewną rolę w szczególnych środkach dochodzenia, pomagać w zapewnieniu lepszej możliwej współpracy władzom państw członkowskich, podejmować działania koordynacyjne w państwach członkowskich, współpracować i wspomagać Europol i EJN, oferować wsparcie logistyczne[524].

* * *

Większość państw podejmuje próby zmierzenia się z kwestią regulacji zachowań w cyberprzestrzeni. Wszystkie wyszczególnione w niniejszej publikacji akty prawne i dokumenty łączy wspólny problem w określeniu kompetencji i uprawnień państw w zakresie regulowania przestrzeni wirtualnej. Szczególnym wyzwaniem jest ustalenie granic jurysdykcji państw, zwłaszcza że część z nich podejmuje kroki w celu znacznego rozszerzenia swojego władztwa jurysdykcyjnego. Spór w tym zakresie wywołuje pytanie o prawo właściwe w przypadku popełnienia cyberprzestępstwa, działań terrorystów w przestrzeni wirtualnej czy kwestiach związanych z codziennym życiem miliona ludzi, czyli handlem elektronicznym czy granicami wolności słowa.

Opisane w niniejszym rozdziale organizacje międzynarodowe podejmują próbę regulowania najbardziej newralgicznych kwestii związanych z działalnością człowieka w cyberprzestrzeni. Organizacją o największym zasięgu jest ONZ, która działając za pomocą swoich wyspecjalizowanych agencji, proponuje rozwiązania w zakresie cyberprzestępczości (UNODC) czy handlu elektronicznego (UNICITRAL). Podmiotem, który może w przyszłości odegrać ważną rolę, jest Forum Zarządzania Internetem (Internet Governance Forum – IGF) będące nowym modelem tworzenia wspólnej polityki na poziomie międzynarodowym. Wprawdzie IGF nie może wydawać decyzji merytorycznych, lecz przedstawianie rekomendacji w formie modelu *soft law* może się sprawdzić w odniesieniu do wyzwań związanych z regulacją cyberprzestrzeni.

Szczególną uwagę należy zwrócić na pracę regionalnych organizacji międzynarodowych oraz ich wkład w tworzenie cyberprawa. Jednym z pierwszych holistycznych aktów prawnych poruszających problem działalności kryminalnej człowieka w cyberprzestrzeni była *Konwencja Rady Europy o cyberprzestępczości*. Przystąpiły do niej państwa również spoza Rady Europy, a wiele krajów nowelizowało krajowe kodeksy karne, wprowadzając penalizację cyberprzestępstw, opierając się na wspomnianym traktacie. Dokument ten zawiera jednak głównie przepisy

materialnoprawne, nie poruszając zagadnienia związanego z pracą dochodzeniowo-śledczą i koniecznej współpracy w zakresie kryminalistyki. Regulacjami o szczególnym znaczeniu są również *Protokół dodatkowy do konwencji o cyberprzestępczości* dotyczący kryminalizacji działań o charakterze rasistowskim i ksenofobicznym popełnianych przy użyciu systemów komputerowych oraz *Konwencja RE o ochronie dzieci przed wykorzystaniem seksualnym i niegodziwym traktowaniem w celach seksualnych*.

Z europejskiego punktu widzenia organizacją międzynarodową o największym oddziaływaniu na prawo krajowe oraz europejską unifikację przepisów jest Unia Europejska będąca liderem w zakresie przyjętych rozwiązań oraz szczegółowości poruszanych kwestii. Inne organizacje międzynarodowe decydują się na uregulowanie jedynie ściśle określonej kwestii takich, jak handel elektroniczny czy cyberprzestępczość. Unia podejmuje próbę regulacji niemal każdego aspektu prawa cyberprzestrzeni – przestępczości, handlu, własności intelektualnej, danych osobowych, wolności słowa. Dzięki wprowadzonym normom europejski rynek jest najbardziej spójny, a internauci łatwiej dochodzą swoich praw. Tym, co negatywnie wpływa na kształt i efektywność unijnego prawa, jest ogromna fragmentaryzacja i różnice w implementacji ustawodawstwa UE do krajowych porządków prawnych. Istnieją obszary, w których widoczna jest potrzeba wprowadzenia jednego dokumentu holistycznego zamiast kilkunastu szczegółowych aktów prawnych (np. w zakresie własności intelektualnej). Wydana kilkanaście lat temu dyrektywa o handlu elektronicznym również powinna zostać znowelizowana, aby odpowiadać wyzwaniom współczesnego e-commerce.

Cyberprzestrzeń, będąc przestrzenią globalną, ponadnarodową i transgraniczną, nie ogranicza się wyłącznie do rozwiązań regionalnych. Wyspecjalizowane jednostki takie, jak NATO coraz wyraźniej zaznaczają problem cyberagresji między państwami, które mogą stanowić element wojny hybrydowej. Obawa ta jest realna jak nigdy wcześniej. Przytoczone przykłady cyberagresji na Estonię i Gruzję wskazują, że oprócz wojen na lądzie, wodzie i w powietrzu w przyszłości pojawią się konflikty również w przestrzeni wirtualnej,

paraliżując systemy bądź dezinformując przeciwnika, dlatego konieczne jest wprowadzenie polityki cyberbezpieczeństwa w krajowych porządkach prawnych.

Nie mniej istotna jest konieczność koordynacji i współpracy działań w zakresie walki z cyberprzestępczością i cyberterroryzmem, np. w kontekście nasilającego się terroryzmu oraz walki z Państwem Islamskim. W organizacjach takich, jak Interpol czy Europol wykształcono wyspecjalizowane jednostki, które mają zapobiec najpoważniejszym cyberprzestępstwom, czyli cyberterroryzmowi, pornografii dziecięcej czy praniu pieniędzy, ścigać i zwalczać je. Tylko skorelowane międzynarodowe działania mogą przynieść oczekiwany skutek. Cyberprzestępcy stają się coraz bardziej pomysłowi, wykorzystują najnowsze techniki i nierzadko kosztowny specjalistyczny sprzęt. Efektywna walka z przestępczością wirtualną powinna rozpocząć się od stałej współpracy, wymiany doświadczeń oraz informowania o zagrożeniach. Niezbędne są również szkolenia dla organów ścigania i sprawiedliwości oraz techników kryminalistycznych w zakresie technik i metod prowadzenia postępowania cyfrowego oraz zbierania i wykorzystania w sądzie dowodów cyfrowych. Instytucją, która może mieć w przyszłości szczególne znaczenie, jest Europejskie Centrum ds. Walki z Cyberprzestępczością, które jest powołane do walki z najpoważniejszymi przestępstwami popełnianymi w cyberprzestrzeni, z przestępczością zorganizowaną, seksualnym wykorzystywaniem dzieci i pornografią dziecięcą oraz ochroną infrastruktury krytycznej Unii Europejskiej.

Nie należy również pominąć wkładu organizacji wyspecjalizowanych podejmujących kroki legislacyjne w celu zapewnienia bezpieczeństwa sieci (ENISA) oraz standaryzowania i regulowania rynku telekomunikacyjnego w tym w zakresie, ochrony przed cyberprzestępczością (ITU). Odzwierciedleniem wolnościowego charakteru cyberprzestrzeni jest organizowanie Światowego Szczytu Społeczeństwa Informacyjnego o elastycznej formule, wskazującego kierunki działań w zakresie budowy społeczeństwa informacyjnego, powszechnego dostępu do informacji oraz Internetu. OECD za pomocą regulacji typu *soft law*

podjęła się wytyczenia kierunku zmian legislacyjnych dotyczących podpisu elektronicznego oraz technicznych i prawnych aspektów handlu elektronicznego.

5

REALIZACJA POLITYKI CYBERBEZPIECZEŃSTWA UNII EUROPEJSKIEJ

Przedmiotem analizy niniejszego rozdziału monografii jest polityka ochrony cyberbezpieczeństwa Unii Europejskiej. Należy zwrócić uwagę na fakt, że Unia Europejska jest podmiotem prawa międzynarodowego, a nie jak dotychczas opiera się na supranarodowości. W tym rozdziale został wyraźnie zdefiniowany podmiot i przedmiot polityki ochrony cyberbezpieczeństwa, a także przedstawione i ocenione instrumenty stosowane przez Unię Europejską w ramach prowadzonej przez nią polityki antyterrorystycznej, w szczególności po wejściu w życie Traktatu z Lizbony.

Analiza realizacji polityki ochrony cyberbezpieczeństwa umożliwi poznanie instrumentów, za pomocą których Unia Europejska realizuje funkcje ochronne, jakie bezpieczeństwo ma spełniać na poziomie zarówno europejskim, jak i państwowym. Jednocześnie została podjęta próba znalezienia odpowiedzi na pytania, w jakim stopniu skuteczność polityki ochrony cyberbezpieczeństwa zależy od rodzaju instrumentów i jakie okoliczności na to wpływają. Zostanie również ukazana zależność problemów bezpieczeństwa wewnętrznego UE, a tym samym polityki ochrony cyberbezpieczeństwa, od poziomu integracji państw członkowskich.

W przypadku Unii Europejskiej mamy do czynienia z przeniesieniem określonych władczych funkcji na poziom europejski. Polityka cyberbezpieczeństwa stanowi jedną z dziedzin polityki Unii Europejskiej i posługuje się różnymi instrumentami służącymi do jej realizacji, dlatego w tym rozdziale dokonano podziału tych działań na odnoszące się do Unii Europejskiej oraz na skierowane na zewnątrz UE. Do tych instrumentów należy zaliczyć: Eurojust, Europol, ENISA, ENA, NIS i decyzje ramowe w sprawie zwalczania cyberterroryzmu oraz działania dotyczące ochrony cyberbezpieczeństwa. Ponadto została podjęta próba odpowiedzi na pytania dotyczące podziału kompetencji w kwestii zwalczania cyberterroryzmu między UE a państwami członkowskimi oraz tego, jak ten podział powinien przebiegać.

5.1
UNIA JAKO PODMIOT POLITYKI OCHRONY CYBERBEZPIECZEŃSTWA

Podmiotem analizowanej polityki ochrony cyberprzestrzeni jest Unia Europejska, która po wejściu w życie Traktatu z Lizbony, na podstawie art. 47 TUE nabyła osobowość prawną, w związku z art. 1 akapit 3 TUE zastąpiła Wspólnotę Europejską i jest jej następcą prawnym. Dużą rolę odgrywają organy Unii Europejskiej, tj. Rada UE, która jest głównym organem decyzyjnym, określa strategiczne interesy i kierunki polityki UE[525], Komisja Europejska, będąca organem wykonawczym UE, oraz Parlament, który razem z Radą pełni funkcję prawodawczą. Nowością było powołanie Wysokiego Przedstawiciela Unii ds. Zagranicznych i Polityki Bezpieczeństwa, tzw. Koordynatora[526] ds. Przeciwdziałania Terroryzmowi[527].

Unia Europejska za pośrednictwem organów stanowi prawo i podejmuje działania, dlatego to właśnie ją w pierwszej kolejności dotykają skutki podjętych decyzji. Stosując odpowiednie instrumenty, UE przeciwdziała działaniom terrorystycznym

podejmowanym przez różne organizacje cyberterrorystyczne. W niniejszym rozdziale przedmiotem badawczym jest polityka antyterrorystyczna realizowana za pomocą jej instrumentów[528].

Należy przypomnieć, że w przypadku państw europejskich polityka cyberbezpieczeństwa miała przede wszystkim charakter wewnętrzny, co spowodowało dwojakiego rodzaju następstwa. Państwa uznawały i w wielu przypadkach nadal uznają, że przeciwdziałanie cyberterroryzmowi należy wyłącznie do ich kompetencji. Współpracę międzynarodową w tym zakresie postrzegają jako konieczną, ale będącą jedynie uzupełnieniem i poszerzeniem zdolności do walki z cyberterroryzmem[529]. Dopiero po wejściu w życie Traktatu z Maastricht polityka cyberbezpieczeństwa znalazła się oficjalnie w III filarze Unii Europejskiej, czyli współpracy międzyrządowej w dziedzinie sprawiedliwości i spraw wewnętrznych. Umiejscowienie tej gałęzi polityki w tym filarze spowodowało, że współpraca od początku często była mało efektywna. Wprawdzie w programie ramowej współpracy w sprawach należących do wymiaru sprawiedliwości i spraw wewnętrznych polityka antyterrorystyczna stała się przedmiotem wspólnego zainteresowania wszystkich państw członkowskich, jednak w pierwszych latach obowiązywania Traktatu z Maastricht Unia Europejska prowadziła politykę nastawioną na konsolidację wewnętrzną, przy pewnym zaniedbaniu stosunków z państwami trzecimi. W obszarze III filaru okazało się, że bez kooperacji z państwami ościennymi UE nie uda się osiągnąć założonych celów. Przesądziły o tym także niewielka rola Komisji Europejskiej i marginalizacja Parlamentu Europejskiego. Panowało przekonanie, że współpraca na poziomie międzyrządowym jest wystarczająca[530]. Od momentu wejścia w życie Traktatu amsterdamskiego i utworzenia strefy wolności, bezpieczeństwa i sprawiedliwości państwa członkowskie wzmocniły środki działań, integrując instrumenty odnoszące się do kontroli na granicach zewnętrznych, azylu i migracji w ramach Wspólnoty oraz zapobiegając i zwalczając przestępczość międzynarodową[531].

Na skutek rozwoju EU justice and home affaires końcem XX w. walka z terroryzmem poprawiła się na poziomie UE w wymiarze instytucjonalno-strukturalnym. Dotychczasowe struktury Trevi zostały w całości włączone w strukturę JHA Council. W rzeczywistości istotną rolę w procesie podejmowania decyzji ministerialnych dotyczących walki z terroryzmem odgrywał art. 36 TUE, stanowiący podstawę prawną funkcjonowania dobrze zakorzenionego już od TUE Komitetu Koordynacyjnego, którego zasadniczym zadaniem była koordynacja zadań państw członkowskich w ramach dawnego III filaru. Komitet (CATS)[532] miał możliwość wpływania na kierunki rozwoju i pomagał w przygotowywaniu prac Rady, gdy miała się ona zająć współpracą policyjną i sądową w sprawach karnych[533]. Komitet (CATS) skupia wyższych urzędników państwowych i Komisje zajmujące się współpracą sądową i policyjną. CATS wydaje również instrukcje Radzie Grupy Roboczej ds. Terroryzmu (WPT), która skupia państwowych i europejskich urzędników Komisji, zajmujących się zwalczaniem terroryzmu w obszarze III filaru. WPT jest odpowiedzialna za opracowanie szczegółów walki z terroryzmem, a kwestie szczegółowe, odnoszące się do współpracy policyjnej oraz współpracy sądowej, zostały omówione i uzgodnione w innych wyspecjalizowanych grupach roboczych Rady[534].

Traktat z Lizbony dokonał rozdziału zadań między UE a państwa w sposób bardziej precyzyjny w porównaniu do dawnych przepisów. Już w art. 4 TFUE stwierdzono, że Unia szanuje podstawowe funkcje państw. Koreluje to częściowo z postanowieniami art. 67 TFUE. Warto przypomnieć, że art. 3 ust. 2 TFUE przewiduje utrzymanie i rozwój Unii jako przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Umiejscowienie w art. 3 ust. 2 TFUE na drugim miejscu celu, jakim jest zapewnienie obywatelom przestrzeni wolności, bezpieczeństwa i sprawiedliwości, tuż po celu, jakim jest wspieranie pokoju, jego wartości i dobrobytu wśród jej narodów, podkreśla również znaczenie, jakie państwa członkowskie nadają współpracy w tym obszarze. Wskazuje też na kolejny etap w rozwoju współpracy w tej materii, obserwowany od lat 70. XX w.[535]

Tradycyjnie zastrzeżono, że w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego pozostaje w szczególności bezpieczeństwo narodowe (art. 4 TFUE), chociaż mogą one między sobą i na swoją odpowiedzialność organizować uznane przez niezastosowane formy współpracy i koordynacji między właściwymi służbami ich administracji odpowiedzialnymi za zapewnienie bezpieczeństwa narodowego (art. 73 TFUE)[536].

Z kolei z art. 24 ust. 1 Traktatu z Lizbony wynika, że wspólna polityka zagraniczna i bezpieczeństwa podlega szczególnym zasadom i procedurom. Jest określana i realizowana przez Radę Europejską stanowiącą jednomyślnie, chyba że traktaty przewidują inaczej. Wspólną politykę zagraniczną i bezpieczeństwa wykonuje Wysoki Przedstawiciel Unii ds. Zagranicznych i Polityki Bezpieczeństwa oraz państwa członkowskie zgodnie z traktatami. Szczególną rolę Parlamentu Europejskiego i Komisji w tej dziedzinie określają traktaty. Ponadto w art. 26 ust. 1 zapisano, że Rada Europejska określa strategiczne interesy Unii, ustala cele oraz określa ogólne wytyczne wspólnej polityki zagranicznej i bezpieczeństwa, łącznie ze sprawami mającymi wpływ na kwestie polityczno-obronne. Podejmuje niezbędne decyzje, a jeśli wymaga tego sytuacja międzynarodowa, przewodniczący Rady Europejskiej zwołuje nadzwyczajne posiedzenie Rady w celu określenia strategicznych kierunków polityki UE w obliczu takiej sytuacji. Zgodnie z art. 28 ust. 1 Traktatu z Lizbony w zw. z art. 43 TUE Unia może tworzyć misje: humanitarne i ratunkowe, wojskowego doradztwa i wsparcia, zapobiegania konfliktom i utrzymywania pokoju, zbrojne służące zarządzaniu kryzysowemu, w tym misje przywracania pokoju i operacje stabilizacji sytuacji po zakończeniu konfliktów[537].

Połączenie polityki zagranicznej z polityką bezpieczeństwa regionu, czyli Unii Europejskiej, stanowi ścisły związek dwóch polityk współzależnych i podporządkowanych jednej instytucji – wysokiemu przedstawicielowi Unii. Z postanowień Traktatu z Lizbony wynika, że rola polityki dotyczącej bezpieczeństwa została podsumowana jednoznacznie w art. 27 TFUE i zawiera zapisy

odnoszące się do Unii jako koalicji i do państw członkowskich. W przypadku podziału kompetencji między Unię a państwa członkowskie istotną rolę odgrywają te przepisy, w których dodano wyraźnie, że:

- środki przyjmowane przez Parlament Europejski i Radę w celu promowania i wspierania działania państw członkowskich w dziedzinie zapobiegania przestępczości nie mogą dotyczyć jakiejkolwiek harmonizacji przepisów ustawowych i wykonawczych państw członkowskich (art. 84 TFUE),
- utrzymano proponowane w Traktacie ustanawiającym Konstytucję dla Europy tzw. hamulce bezpieczeństwa,
- stosowanie środków przymusu w przypadku działań operacyjnych prowadzonych przez Europol[538] wspólnie z organami państw członkowskich zastrzeżono do wyłącznej kompetencji organów państwowych (art. 88 ust. 3 TFUE).

Zgodnie z obecnym art. 75 Traktatu o Unii Europejskiej i o funkcjonowaniu Unii Europejskiej polityka antyterrorystyczna, w tym ochrona cyberprzestrzeni, jest oparta na zasadzie współdecydowania. Podstawą prawną procedury współdecydowania (kodecyzji) jest art. 294 TL. Organami współdecydującymi o przyjęciu lub odrzuceniu aktu prawnego są Rada i Parlament Europejski, natomiast inicjatywa ustawodawcza należy do Komisji[539]. Głównym założeniem tej zasady jest uniknięcie podejmowania decyzji[540] bez uzgodnienia wspólnego stanowiska między tymi dwoma ciałami a Komisją Europejską[541]. Takie rozwiązanie okazało się sukcesem w przypadku rozbieżnych często stanowisk poszczególnych grup interesów pojawiających się na poszczególnych etapach procesu legislacyjnego[542].

W art. 67 TFUE zapisano, że Unia jest przestrzenią wolności, bezpieczeństwa i sprawiedliwości, mającą na celu poszanowanie praw podstawowych oraz różnych systemów i tradycji prawnych państw członkowskich. Unia ma także dołożyć wszelkich starań, aby zapewnić wysoki poziom bezpieczeństwa za pomocą środków zapobiegających przestępczości, rasizmowi i ksenofobii oraz

zwalczających te zjawiska oraz przy użyciu środków służących koordynacji i współpracy organów policyjnych i sądowych, a także innych właściwych organów, również za pomocą wzajemnego uznawania orzeczeń sądowych w sprawach karnych i, w miarę potrzeby, przez zbliżanie przepisów karnych. Jeżeli natomiast wymaga tego realizacja celów, o których mowa w art. 67 TFUE, w odniesieniu do zapobiegania terroryzmowi i działalności powiązanej oraz zwalczania tych zjawisk, to Parlament Europejski i Rada, stanowiąc w drodze rozporządzeń zgodnie ze zwykłą procedurą prawodawczą, określają ramy środków administracyjnych dotyczących przepływu kapitału i płatności takich, jak zamrożenie funduszy, aktywów finansowych lub zysków z działalności gospodarczej, które należą do osób fizycznych lub prawnych, grup lub innych podmiotów innych niż państwa, są w ich posiadaniu lub dyspozycji (obecny art. 75 TFUE[543]).

W myśl art. 71 TFUE pozostawiono w ramach Rady stały komitet ds. zapewnienia wspierania i wzmacniania współpracy operacyjnej wewnątrz Unii w zakresie bezpieczeństwa wewnętrznego[544]. Z art. 73 TFUE wynika z kolei, że państwa członkowskie UE mogą niezależnie organizować między sobą i na swoją odpowiedzialność, uznane przez nie za stosowne formy współpracy i koordynacji między właściwymi służbami administracji odpowiedzialnymi za zapewnienie bezpieczeństwa narodowego.

Do tej pory z Parlamentem Europejskim należało jedynie konsultować prawnie wiążące działania w zakresie wymiaru sprawiedliwości i spraw wewnętrznych. Istotną zmianą w porównaniu z dotychczasowym stanem prawnym jest modyfikacja procedury przyjmowania tych norm minimalnych – na mocy TFUE są one ustalane w formie dyrektyw przyjmowanych w zwykłej procedurze prawodawczej przez Parlament Europejski i Radę UE[545]. W konsekwencji, od momentu wejścia w życie TL zasadą stała się harmonizacja dyrektyw przyjmowanych przez Radę UE kwalifikowaną większością głosów w zwykłej procedurze prawodawczej, podczas gdy w poprzednim stanie prawnym harmonizacja prawa karnego odbywała się w drodze decyzji

ramowych przyjmowanych jednomyślnie. Gwarantuje to Parlamentowi Europejskiemu istotny wpływ na kształt przyjmowanego aktu prawnego. Jest to więc zmiana dość radykalna w porównaniu z dotychczas obowiązującym stanem prawnym, ponieważ państwa członkowskie co do zasady zrzekły się przysługującego im do tej pory prawa weta i zgodziły się, że dyrektywa może być przyjęta wbrew stanowisku państw członkowskich, które nie mają mniejszości blokującej. Rezygnacja z przyjmowania tych aktów w Radzie jednomyślnie na rzecz głosowania kwalifikowaną większością głosów została obwarowana dwoma szczególnymi mechanizmami „elastyczności". Należy podkreślić, że zmiana formy aktu prawnego pozwala spodziewać się zwiększenia efektywności środków harmonizujących w prawie państwowym państw członkowskich. Trybunał będzie miał pełną jurysdykcję przede wszystkim w odniesieniu do procedury o stwierdzenie uchybienia zobowiązaniom państwa członkowskiego, która jest wszczynana w wyniku skargi Komisji Europejskiej i stanowi skuteczny mechanizm egzekwowania implementacji dyrektyw[546].

Istotne było wprowadzenie w art. 82 ust. 2 TL możliwości harmonizacji przepisów z zakresu prawodawstwa karnego przez normy minimalne o wymiarze transgranicznym, z uwzględnieniem różnic między tradycjami a systemami prawnymi poszczególnych państw członkowskich. Państwa, niezależnie od minimalnych standardów przewidzianych w normach, mogą utrzymywać lub ustanawiać wyższe poziomy ochrony osób. Należy dodać, że zwykła procedura prawodawcza przewidziana w TL jest wzorowana na dotychczasowej procedurze współdecydowania (określonej w art. 251 TWE), która gwarantuje Parlamentowi Europejskiemu istotny wpływ na kształt przyjmowanego aktu prawnego[547],[548].

Zgodnie z art. 83 ust. 2 TFUE, jeżeli zbliżanie przepisów ustawowych i wykonawczych państw członkowskich w sprawach karnych okaże się niezbędne w celu zapewnienia skutecznego wprowadzania w życie polityki Unii w dziedzinie, która stała się przedmiotem środków harmonizujących, dyrektywy mogą ustanowić

normy minimalne, odnoszące się do określania przestępstw oraz kar w danej dziedzinie. Dyrektywy te przyjmuje się zgodnie ze zwykłą lub specjalną procedurą prawodawczą, taką jak procedura stosowana do przyjmowania stosownych środków harmonizujących[549].

Jeżeli incydent nosi znamiona szpiegostwa cybernetycznego lub ataku inicjowanego przez państwo albo ma wpływ na bezpieczeństwo państwa, krajowe organy bezpieczeństwa i obrony ostrzegają swoich odpowiedników, że są celem ataku, by mogli się odpowiednio bronić. Zostaną uruchomione mechanizmy wczesnego ostrzegania oraz w razie potrzeby procedura zarządzania kryzysowego i inne procedury. Szczególnie poważny incydent lub atak w zakresie bezpieczeństwa cybernetycznego może stanowić wystarczającą podstawę, by państwo członkowskie powołało się na klauzulę solidarności UE (art. 222 TFUE)[550]. Jeżeli incydent wydaje się prowadzić do naruszenia danych osobowych, należy powiadomić krajowe organy ds. ochrony danych lub krajowy organ regulacyjny, zgodnie z dyrektywą 2002/58/WE[551]. W przypadku wystąpienia incydentów i ataków cybernetycznych przydatne będą sieci kontaktów oraz wsparcie ze strony partnerów międzynarodowych, które może obejmować zastosowanie środków technicznych ograniczających wpływ incydentu, prowadzenie dochodzeń oraz uruchomienie mechanizmów reagowania w sytuacjach kryzysowych.

Zgodnie z art. 85 TFUE współpraca w sprawach karnych jest uzupełniona działalnością Eurojustu i Prokuratury Europejskiej. Naczelnym zadaniem Eurojustu[552] jest wspieranie oraz wzmacnianie koordynacji i współpracy między państwowymi organami śledczymi i organami ścigania w odniesieniu do poważnej przestępczości, która dotyka dwóch lub więcej państw lub która wymaga wspólnego ścigania na podstawie przeprowadzanych operacji i informacji przekazywanych przez organy państw członkowskich i Europol[553].

Z art. 88 ust. 1 TFUE wynika, że zadaniem Europolu[554] jest wspieranie i wzmacnianie działań organów policyjnych oraz innych organów ścigania państw unijnych, jak również ich wzajemnej współpracy w celu zapobiegania i zwalczania poważnej przestępczości na terenie dwóch lub więcej państw, terroryzmu oraz

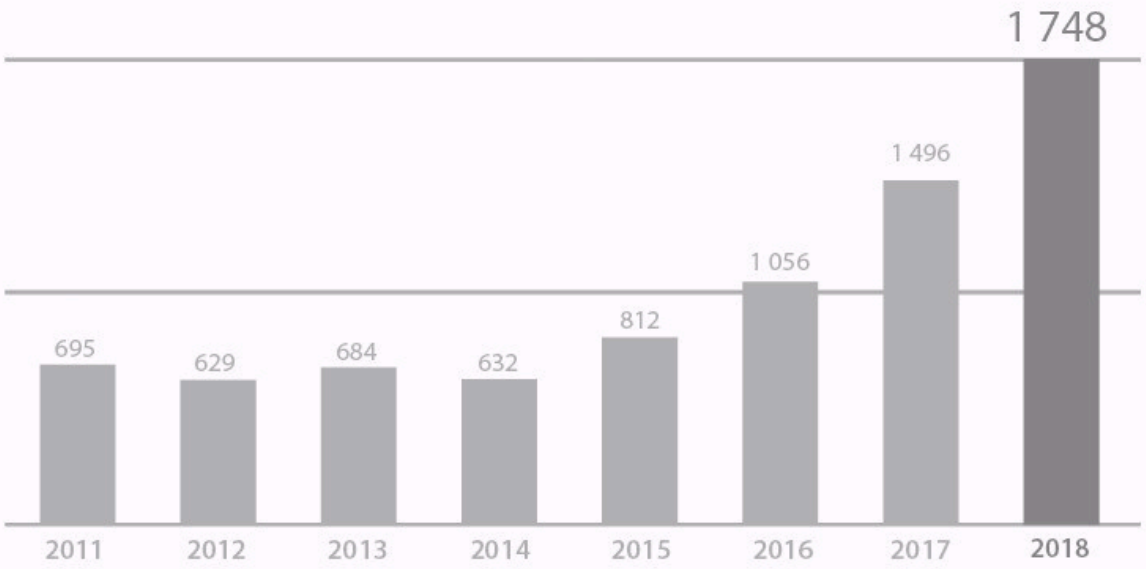
innych form przestępczości naruszających wspólny interes objęty polityką UE.

Z danych statystycznych Europolu przedstawionych na rys. 5.1 wynika, że cyberterroryzm jest obecnie drugim co do wielkości zagrożeniem w Unii Europejskiej tuż po terroryzmie. Od wystąpienia kryzysu migracyjnego UE w 2015 r. obserwuje się także wzrost operacji mających na celu zwalczanie tego zjawiska.

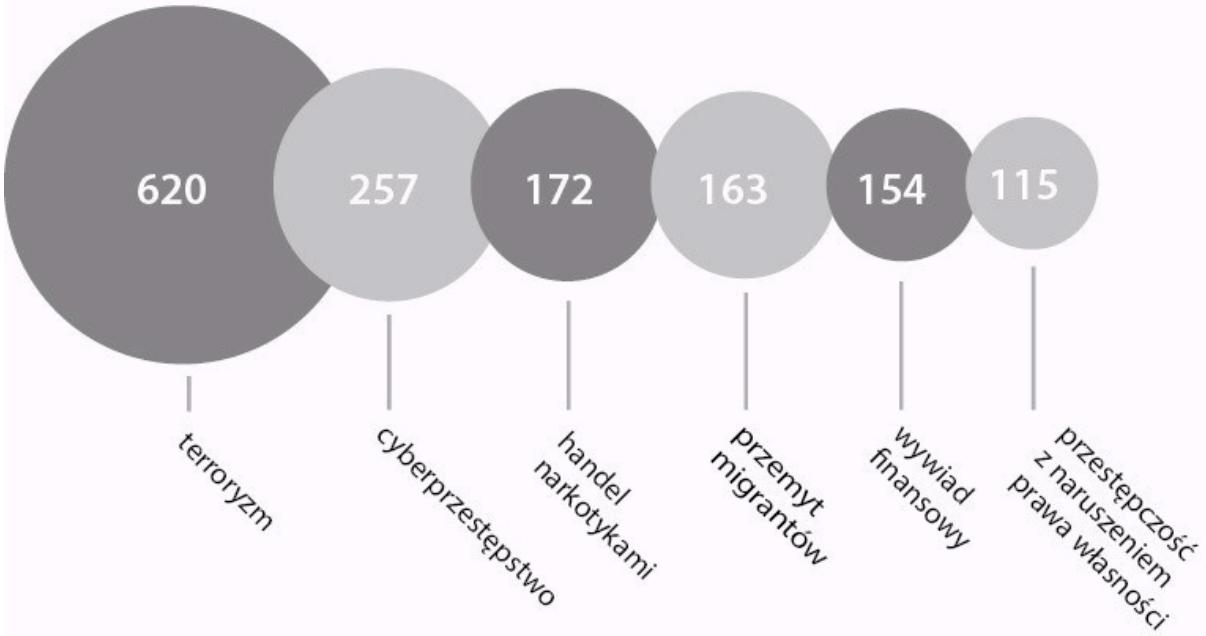
Momentem zwrotnym w realizacji polityki cyberbezpieczeństwa był rok 1999, kiedy wydano *Zieloną Księgę Public Sector Information: a Key Resource for Europe* i wskazano korzyści z bycia społeczeństwem informacyjnym w obszarze służb publicznych. Dlatego jako priorytet Unia Europejska przyjęła umożliwienie powszechnego dostępu do Internetu. Taki plan został opracowany na specjalnym posiedzeniu Rady Europejskiej 23–24 marca 2000 r. w Lizbonie pn. *Strategia Lizbońska*. Sporządzono go na dwóch płaszczyznach: gospodarczej i społecznej. Płaszczyzna społeczna opierała się na koncepcji Luca Soete'a, który uznał społeczeństwo informacyjne za „społeczeństwo, które właśnie się kształtuje, w którym technologie gromadzenia oraz transformacji informacji i danych są powszechnie dostępne po niskich kosztach".

1 748

przeprowadzone zamachy



Główne obszary zbrodni



RYSUNEK 5.1 Liczba przeprowadzonych ataków w terrorystycznych w latach 2011–2018 z podziałem na kategorie

Źródło: Raport: Europol in brief 2018, s. 9.

Podczas kolejnego szczytu europejskiego w Feira w 2000 r. został przyjęty plan *eEurope 2002 – An Information Society for All*. Dokument ten wskazywał konieczność szybkiego, taniego, powszechnego rozwoju Internetu oraz popularyzacji sieci wirtualnej. Kolejny plan rozwoju społeczeństwa informacyjnego, rozumianego jako strategiczny element budowy gospodarki opartej na wiedzy, przedstawiono w 2001 r. w Göteborgu pn. *eEurope + 2003: A Cooperative Effort to Implement the Information Society in Europe – Action Plan*. Założono w nim pobudzenie modernizacji gospodarek państw kandydujących do Unii przez wykorzystanie narzędzi i technologii społeczeństwa informacyjnego. Na szczycie w Sewilli 21–22 czerwca 2002 r. przyjęto kolejny planu rozwoju społeczeństwa informacyjnego *eEurope 2005: An Information Society for All – Action Plan*. Państwa członkowskie UE zobowiązały się do realizacji następujących zadań:

- rozwój usług elektronicznych typu: e-learning, e-government, e-health,
- tworzenie dynamicznego środowiska do rozwoju gospodarki elektronicznej,
- zapewnienie powszechnego dostępu do Internetu szerokopasmowego,
- budowa systemu bezpieczeństwa infrastruktury informacyjnej.

W dokumencie Komisji Europejskiej z 2005 r. *i2010 – European Information Society for Growth and Employment* państwa członkowskie UE uznały, że wiedza i innowacje są motorem zrównoważonego wzrostu. Stwierdzono, że budując jednolitą przestrzeń informacyjną, konieczne jest odniesienie się do czterech głównych wyzwań związanych z konwergencją cyfrową: szybkości (dostęp do szybkich usług szerokopasmowych, ułatwiających dostęp do zawartości multimedialnej, czyli np. wideo w wysokiej rozdzielczości), zawartości multimedialnej (poprawa sytuacji

ekonomicznej i prawnej sprzyjającej powstawaniu nowych usług i zawartości online), interoperacyjności (ulepszenie urządzeń i platform, stworzenie usług umożliwiających komunikowanie się między różnymi platformami) oraz bezpieczeństwa (lepsze zabezpieczenie przed awariami technologicznymi, oszustwami i szkodliwą zawartością).

Jak ustalono w programie haskim[555], przy zachowaniu bezpieczeństwa narodowego państwa członkowskie będą także skoncentrowane na bezpieczeństwie Unii jako całości, która będzie wspierać wysiłki państw członkowskich, aby zakłócić działania terrorystów przez zachęcanie państw do wymiany informacji i danych wywiadowczych zarówno na poziomie Unii, jak i bezpośrednio między państwami członkowskimi. Wymiana danych ma służyć dostarczeniu wspólnej analizy zagrożenia terrorystycznego, a także wzmocnieniu współpracy operacyjnej w egzekwowaniu prawa. Na poziomie państwowym właściwe władze muszą posiadać niezbędne narzędzia do zbierania i analizowania danych wywiadowczych. Europejski proces wzajemnej oceny już wzmocnionych państwowych uzgodnień w niektórych krajach nadal może prowadzić do skuteczniejszej polityki antyterrorystycznej i prawodawstwa w zakresie całej swojej działalności. Wypracowanie wspólnych zasad i zrozumienie podstawowych zagrożeń jest niezbędne w rozwoju wspólnej polityki antyterrorystycznej. Wspólne Centrum Sytuacyjne odgrywa ważną rolę w dostarczaniu ocen i analiz strategicznego zagrożenia terrorystycznego przeprowadzanych na podstawie danych z zakresu bezpieczeństwa narodowego i agencji wywiadowczych oraz Europolu[556].

Za priorytetowe należy uznać prace w kierunku modelu europejskiego wywiadu kryminalnego. W odniesieniu do kwestii prawa karnego ustawodawstwo państwowe musi czasami być zbliżone, dlatego należy opracować minimalne standardy proceduralne, by w ten sposób wzmocnić wzajemne zaufanie między państwami członkowskimi[557]. Do wejścia w życie Traktatu z Lizbony za sukces w obszarze zwalczania terroryzmu i cyberterroryzmu należy uznać następujące akty prawne:

- Konwencja z 1995 r. o utworzeniu Europejskiego Urzędu Policji (Europol)[558].
- Decyzja ramowa Rady z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu[559] aresztowania i procedury wydawania osób między państwami członkowskimi.
- Decyzja ramowa Rady z dnia 13 czerwca 2002 r. w sprawie wspólnych zespołów dochodzeniowo-śledczych[560].
- Decyzja Rady z dnia 28 lutego 2002 r. ustanawiająca Eurojust[561].
- System Informacji Schengen[562].
- Decyzja Rady z dnia 20 września 2005 r. w sprawie wymiany informacji i współpracy dotyczącej przestępstw terrorystycznych[563].
- Dyrektywa Parlamentu w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowaniu terroryzmu z dnia 26 października 2005 r.[564].
- Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[565], która została uchwalona w celu stworzenia generalnych ram ochrony danych osobowych w EWG.
- Dyrektywa 2002/22/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie usługi powszechnej oraz związanych z sieciami i usługami łączności elektronicznej praw użytkowników (dyrektywa o usłudze powszechnej)[566], zgodnie z art. 23 państwa członkowskie są zobowiązane do podjęcia koniecznych środków w celu zapewnienia integralności stacjonarnej publicznej sieci telefonicznej oraz w przypadku załamania sieci w wyniku katastrofy lub w przypadku działania siły wyższej, dostępności usług stacjonarnej publicznej sieci telefonicznej i publicznie dostępnych usług telefonicznych, a działania podejmowane przez przedsiębiorstwa świadczące stacjonarne publicznie dostępne usługi telefoniczne w tym zakresie powinny się mieścić w granicach rozsądku, w celu zapewnienia nieprzerwanego dostępu do służb ratunkowych.

- Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 12 lipca 2002 r. o prywatności i łączności elektronicznej dotyczącej m.in. bezpieczeństwa publicznych sieci łączności elektronicznej[567].
- Decyzja ramowa 2005/222/WSiSW Rady z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[568].

Komisja uznała, że należy podjąć działania zmierzające do utworzenia spójnego i kompleksowego mechanizmu oceny polityki Unii Europejskiej w dziedzinie wolności, bezpieczeństwa i sprawiedliwości, w duchu partnerstwa z państwami członkowskimi i instytucjami UE. Podobnie jak w Tampere, Komisja w ramach programu haskiego i jego planu działania postanowiła naprawić istniejące mechanizmy monitorowania i oceny oraz zaspokoić potrzeby informowania wszystkich zainteresowanych stron o realizacji i wynikach polityki wzmacniania wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej. Oprócz monitorowania tego procesu po raz pierwszy położono nacisk na monitorowanie państwowych realizacji tych polityk. Wynika to ze wstępnej oceny, że mimo postępu osiągniętego przez Unię w ramach „uwspólnotowienia" polityki wolności, bezpieczeństwa i sprawiedliwości, w obszarze współpracy sądowej w sprawach cywilnych nastąpiło jednak opóźnione przyjęcie priorytetu polityki w ramach programu haskiego ze względu na kwestie, które dotyczą pierwszego etapu europejskiego systemu azylowego. Na poziomie państwowym szczególnie problematyczne pozostają jednak przyjęcie i realizacja współpracy policyjnej i sądowej w sprawach karnych („trzeci filar").

Plan Rady i Komisji wdrażający program haski w sprawie wzmocnienia wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej[569] miał się odnosić do pracy Rady i Komisji na lata 2004–2009. Zawiera on harmonogram przyjęcia i wprowadzenia w życie zawartych w nim działań w celu zrealizowania priorytetów i celów, którymi są wzmacnianie wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej[570]. W komunikacie Komisji

przyjęto „Dziesięć priorytetów na najbliższe pięć lat. Partnerstwo na rzecz odnowy europejskiej w dziedzinie wolności, bezpieczeństwa i sprawiedliwości”[571]. Te propozycje legislacyjne, dokumenty konsultacyjne (zielone karty) oraz raporty zostały opracowane, aby w efektywny sposób uzyskać praktyczny rezultat programu haskiego.

Program haski ustanowił, że od 1 stycznia 2008 r. wymiana informacji w zakresie ścigania podlega zasadzie „dostępności”, co oznacza, że na obszarze całej Unii Europejskiej jakakolwiek służba ścigania jednego z państw członkowskich, potrzebująca pewnych informacji do celów wykonywania swoich zadań, może uzyskać je od innego państwa członkowskiego. Program haski podkreśla, że w celach zapobiegawczych dotyczących zwalczania terroryzmu, państwa członkowskie nie mogą ograniczyć swojej działalności do utrzymania własnego bezpieczeństwa, lecz powinny ją skierować na utrzymanie bezpieczeństwa całej Unii[572].

W maju 2005 r. ministrowie siedmiu państw (Niemcy, Hiszpania, Francja, Luksemburg, Holandia, Austria i Belgia) podpisali Schengen III, czyli konwencję z Prüm. Schengen III dotyczy ścisłej współpracy transgranicznej między państwami w zakresie wymiany danych poufnych (takich jak DNA, odciski palców, informacje o pojeździe i osobowych oraz nieosobowe informacje w celu zapobiegania terroryzmowi i cyberterroryzmowi) oraz w zakresie bezpieczeństwa imprez sportowych i masowych. Należy podkreślić, że konwencja z Prüm nie jest częścią dorobku Schengen i została podpisana poza ramami UE[573].

Jedno z ważniejszych spotkań Rady UE ds. WSiSW odbyło się 1–2 grudnia 2005 r. Na posiedzeniu tym przyjęto istotny dla polityki antyterrorystycznej UE dokument *Strategia Unii Europejskiej w zakresie zwalczania terroryzmu* (*The European Union Counter-Terrorism Strategy*)[574]. Podkreślono w niej potrzebę walki z terroryzmem, ochrony obywateli i infrastruktury oraz zmniejszenia podatności na ataki, m.in. przez poprawę bezpieczeństwa granic, transportu i infrastruktury krytycznej, zapobiegania terroryzmowi na terenie całej UE i na świecie przez utrudnianie planowania ataków i komunikacji terrorystom, uniemożliwianie dostępu do

finansowania organizacji terrorystycznych i ataków, minimalizowania skutków ataku terrorystycznego.

Na szczycie w Lac 11–13 maja 2006 r. potępiono wszelkie akty terroru, finansowanie i wspieranie terroryzmu oraz podburzanie do aktów cyberterrorystycznych. Podkreślono potrzebę współpracy w celu zapobiegania terroryzmowi we wszystkich jego formach i przejawach, zwalczania i eliminowania go. Zwrócono uwagę na fakt, że akty terroryzmu negatywnie wpływają na korzystanie z praw człowieka i podstawowych wolności, stanowią bowiem bezpośrednie zagrożenie dla praworządności, osłabiają rozwój gospodarczy i społeczny. Uznano, że państwa członkowskie mają obowiązek chronić swoich obywateli, prawa człowieka, podstawowych wolności, a uprawnienia te muszą być w pełni respektowane podczas walki z terroryzmem. Unia zadeklarowała również pełne poparcie realizacji wszystkich zobowiązań wynikających z instrumentów prawnych ONZ do zwalczania terroryzmu, szczególnie rezolucji nr 1373, 1566, 1624 oraz innych stosownych rezolucji[575].

Na podstawie komunikatu Komisji do Rady i Parlamentu Europejskiego[576] została opracowana i przyjęta przez Radę w lipcu 2006 r. realizacja programu haskiego „przyszłe działania" składająca się z trzech głównych części:

- najważniejszych informacji na temat walki z terroryzmem,
- propozycji dotyczących sposobu realizacji kluczowych wiadomości do różnych odbiorców,
- wspólnego leksykonu, który z biegiem czasu został rozszerzony.

Strategia miała wykorzystać komunikat UE, wartości i politykę w celu zapobiegania terroryzmowi, jednak nie jest wyłącznie związana z komunikatem w sprawie walki z terroryzmem. Powinna być stosowana w kontekście komunikacji UE ze względu na wiele tematów, które mogą mieć wpływ na procesy radykalizacji, takich jak integracja, prawa człowieka, praworządność, pomoc rozwojowa itp. Niniejszy komunikat oraz trzy inne komunikaty przyjęte równolegle[577] są odpowiedzią Komisji Europejskiej na zaproszenie Rady Europejskiej „do raportu w 2006 r. w sprawie poczynionych

postępów i zaproponowania koniecznych uzupełnień programu". Obszarami, których to dotyczy, są:

- prawa podstawowe i obywatelstwa,
- stworzenie drugiego etapu azylu,
- zarządzanie migracją,
- zintegrowane zarządzanie granicami zewnętrznymi oraz interoperacyjność systemów informatycznych,
- wzajemne uznawanie w sprawach cywilnych i karnych,
- dostęp do informacji niezbędnych do zwalczania terroryzmu i przestępczości zorganizowanej,
- przyszłość Europolu[578].

Komisja Europejska wykazała zainteresowanie kwestią rozsyłania niechcianej korespondencji e-mailowej w postaci spammingu i phishingu jeszcze w listopadzie 2006 r., wystosowując do Rady Unii Europejskiej, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów komunikat poświęcony zwalczaniu spamu, oprogramowania szpiegowskiego i złośliwego oprogramowania[579].

Zwrócono się ponadto do wszystkich państw, aby nie zezwalały na bezpieczną przystań dla terrorystów i podejmowały ściganie domniemanych terrorystów lub szybko rozpatrywały wnioski o ekstradycję osób podejrzanych o popełnienie aktów terrorystycznych zgodnie z prawem państwowym i międzynarodowym, w tym na podstawie umów dwustronnych. Zwrócono się także z prośbą do wszystkich państw, aby wszystkie ratyfikowały konwencje i protokoły odnoszące się do terroryzmu[580].

W komunikacie Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 2007 r. *W kierunku ogólnej strategii zwalczania cyberprzestępczości*[581] termin „cyberprzestępczość" został zdefiniowany jako „czyny zabronione dokonane za pomocą lub skierowane przeciwko sieci łączności elektronicznej i systemom informatycznym". Należy zauważyć, że prawne instrumenty służące zapobieganiu cyberterroryzmowi i zwalczaniu go mają różny

charakter: część z nich należy do sfery prawa administracyjnego, większość jednak do obszaru prawa karnego[582].

Należy podkreślić, że na poziomie Unii Europejskiej od dłuższego czasu analizowano korzyści wynikające z rozwoju społeczeństwa informacyjnego, wskutek czego już w 2010 r. w dokumencie *Europejska agenda cyfrowa*[583] określono wiele działań w dziedzinie praw autorskich, mających na celu otwarcie dostępu do treści w ramach *Strategii na rzecz osiągnięcia dynamicznego jednolitego rynku cyfrowego*, co znalazło kontynuację w kolejnych dokumentach, w tym m.in. w *Strategii jednolitego rynku cyfrowego dla Europy*[584] czy *Otwartej i bezpiecznej Europie dla dobra i ochrony obywateli* wraz z planem działania służącym jego realizacji.

Warto odnieść się do komunikatu Komisji Europejskiej dotyczącego realizacji założeń programu sztokholmskiego. W dokumencie tym, w rozdziale *Europa, która chroni,* poświęcono uwagę podniesieniu poziomu ochrony obywateli i przedsiębiorstw w cyberprzestrzeni przez:

- zwiększenie zdolności operacyjnej zwalczania cyberprzestępczości (UE utworzyła Europejskie Centrum ds. Walki z Cyberprzestępczością – EC3 przy biurze Europolu, w związku z czym, o ile to możliwe, zaleca utworzenie centrów ds. walki z cyberprzestępczością we wszystkich państwach członkowskich),
- kontynuację współpracy ze Stanami Zjednoczonymi w ramach wspólnie utworzonego światowego sojuszu przeciwko niegodziwemu traktowaniu dzieci w Internecie w celach seksualnych,
- wdrożenie uzgodnionych przez UE zaostrzonych przepisów mających na celu zwalczanie cyberprzestępczości,
- zacieśnienie współpracy z sektorem prywatnym,
- ustalenie jurysdykcji w cyberprzestrzeni, m.in. dzięki ratyfikowaniu konwencji Rady Europy o cyberprzestępczości przez państwa, które jeszcze tego nie zrobiły.

Odnosząc się do kolejnych zagadnień, które powinny być regulowane przez politykę w zakresie cyberbezpieczeństwa, wymieniono zagadnienia związane z cyberkonfliktami. Pozornie może się wydawać, że problematyka ścigania sprawców kradzieży własności intelektualnej w Internecie znajduje się obecnie poza kręgiem zainteresowania Unii Europejskiej, co pośrednio potwierdza np. przyjęta w 2011 r. strategia *Jednolity rynek w obszarze praw własności intelektualnej, w której brak jest odpowiednich zapisów*.

Zarówno ochrona cyberprzestrzeni, jak i walka z terroryzmem należą do istotnych zadań Unii i powinny być rozpatrywane na szczeblu europejskim. Odpowiedzialność za akty terroryzmu oraz legislację spoczywa na państwach członkowskich, ponieważ są to sprawy, które stanowią przedmiot wspólnego zainteresowania. Państwa członkowskie deklarowały utworzenie wspólnej polityki i prawa unijnego w tym zakresie, lecz kroki w tym kierunku zostały przedsięwzięte dopiero wraz z podpisaniem Traktatu amsterdamskiego. To, co udało się osiągnąć w okresie przed Traktatem z Maastricht, to międzyrządowa współpraca na pewnych szczeblach. Oczywiście najważniejszym międzyrządowym porozumieniem było porozumienie z Schengen, które wprowadziło wspólne środki kontroli granicznej. Wraz z wejściem w życie Traktatu z Maastricht sprawy antyterrorystyczne stały się częścią regulacji. Zostały one jednak umieszczone w III filarze, co oznaczało, że instytucje wspólnotowe nie miały nad nimi kontroli.

Należy podkreślić i zgodzić się ze stanowiskiem M. Grajny[585], że wiele zbędnych dokumentów powstało w wyniku instytucjonalnego wyścigu między Radą UE a Komisją, ponieważ oba te organy chciały zaprezentować swoje zaangażowanie w politykę antyterrorystyczną. Zarówno międzyrządowy charakter III filaru, jak i brak zaufania między państwami członkowskimi osłabiły działania antyterrorystyczne. Walka z terroryzmem była usytuowana w III filarze do momentu wejścia w życie Traktatu z Lizbony, czyli opierała się na zasadzie jednomyślnego współdziałania państw, co oznaczało, że brak współpracy przy podejmowaniu działań w ramach różnych filarów był poważnym podważaniem polityki antyterrorystycznej i

stanowił przeszkodę jej realizacji jako całości. Poza tym wykluczenie Parlamentu Europejskiego i Trybunału Sprawiedliwości[586] oraz brak przejrzystości w procesie podejmowania decyzji utrudniały skuteczną współpracę między państwami członkowskimi. Dopiero wprowadzenie nowego systemu podejmowania decyzji w Radzie od 2014 r. na zasadzie większości kwalifikowanej przewiduje niemal całkowite odejście od jednomyślnego podejmowania decyzji w ramach współpracy policyjnej i sądowej w sprawach karnych, natomiast w ramach polityki zagranicznej z udziałem Unii będzie wymagana jednomyślna zgoda. Nadal potrzeba jednak co najmniej dziewięciu państw członkowskich do ustanowienia wzmocnionej współpracy na podstawie danego projektu dyrektywy (art. 329 TFUE). Konsekwencją przejścia do podejmowania decyzji w Radzie kwalifikowaną większością głosów jest to, że w sprawach współpracy sądowej, w sprawach karnych i współpracy policyjnej wprowadzono szczególne „wentyle bezpieczeństwa", które polegają na możliwości przeniesienia dyskusji we wskazanych w Traktacie sytuacjach na poziom Rady i Parlamentu.

Zwalczanie cyberterroryzmu wymaga wspólnej strategii UE, a wobec globalizacji zarówno terroryzmu, jak i gospodarczej działania na skalę państwową lub współpraca międzyrządowa państw członkowskich w ramach UE przestają wystarczać. Konieczne jest więc sprecyzowanie międzynarodowej strategii w tym zakresie[587].

18 kwietnia 2008 r. osiągnięto zgodę polityczną na poziomie Rady dotyczącą wniosku w sprawie decyzji ustanawiającej Europol. Decyzja ta przewiduje przyznanie Europolowi statusu agencji UE i zastąpienie finansowania międzyrządowego dotacją wspólnotową.

Są co najmniej cztery czynniki, które sprawiają, że konsensus polityczny między państwami członkowskimi jest nieco mniejszy, niż wskazują na to oficjalne deklaracje. Pierwszym są różnice w państwowych doświadczeniach z terroryzmem, percepcja zagrożeń jest inna w państwach członkowskich, które były zaangażowane w przewlekłą walkę z cyberterroryzmem, np. Estonii, Francji, Wielkiej Brytanii, Holandii czy Niemczech, a inna w państwach, które zagrożenia cyberterrorystycznego doświadczyły tymczasowo,

a nawet prawie wcale. To sprawia, że trudniej jest Radzie osiągnąć wspólne priorytety i programy działania. Drugim czynnikiem są różnice w możliwościach państw członkowskich, które dotyczą także wyspecjalizowanych struktur organizacyjnych, szkoleń i wyposażenia. Niektóre państwa członkowskie, np. Wielka Brytania, mają ugruntowaną zintegrowaną strukturę mającą na celu ochronę cyberprzestrzeni, która wykracza poza granice ministerstw (spraw wewnętrznych i obrony). Angażują też skutecznie policję, siły zbrojne i służby wywiadowcze w te działania. Inne państwa natomiast nie wyszły poza małe dochodzenia i jednostki operacyjne[588]. Kolejny czynnik stanowi pojawienie się nieformalnych, dwustronnych[589] i wielostronnych stosunków współpracy, który często wiąże się z udziałem państw spoza UE, takich jak USA. Władze wykonawcze w państwach członkowskich nadal preferują „sprawdzone" stosunki współpracy zamiast kłopotliwych często „nowych" struktur współdziałania z udziałem wszystkich państw członkowskich. Dotyczy to również wymiany informacji poufnych. Czwartym czynnikiem są rozbieżne stanowiska polityczne i prawne. Ogólnie można przyjąć wysoki stopień zgodności państw członkowskich dotyczący stworzenia wspólnego frontu w walce z cyberterroryzmem, jeśli jednak chodzi o podejmowanie decyzji w sprawie wspólnych działań, różnice te nadal pozostają widoczne.

Walkę z cyberterroryzmem można podzielić na dwa rodzaje. Pierwszy z nich to walka doraźna – walka z terrorystami oraz organizacjami terrorystycznymi. To sposób mało skuteczny, nie można bowiem wyeliminować wszystkich cyberterrorystów. Można to porównać do zwalczania objawów choroby bez usuwania jej przyczyn. Drugim, skuteczniejszym sposobem jest likwidowanie przyczyn cyberterroryzmu, u którego podstaw leży zwykle niewiedza społeczna połączona z przekonaniem, że Internet jest „bezpieczny". Likwidowanie przyczyn można przeprowadzić m.in. przez edukację lub kampanię uświadamiającą w zakresie cyberbezpieczeństwa[590].

Plany UE opisano w *Ramach polityki UE w zakresie cyberobrony*, przyjętych w listopadzie 2014 r., w których określono pięć

priorytetów w zakresie cyberobrony w kontekście WPBiO. Głównym celem jest wspieranie współpracy państw członkowskich na szczeblach politycznym, technicznym i prawnym. Ważny jest także zapis, który podkreśla, że UE wyraża silną wolę „dalszej współpracy z NATO w zakresie cyberobrony”[591]. W przyszłości UE może wykorzystywać zasoby oraz potencjał NATO, tak jak to uczyniła, przejmując operacje wojskowe Sojuszu na Bałkanach lub współpracując z NATO przy projektach dotyczących zwalczania piractwa oraz przeciwdziałając zjawisku handlu ludźmi.

Globalna strategia UE na rzecz polityki zagranicznej i bezpieczeństwa została przyjęta przez Radę Europejską 28 czerwca 2016 r.[592] Określiła ona wspólne interesy UE i państw członkowskich. Wskazała następujące priorytety:

- bezpieczeństwo Unii,
- sąsiedztwo,
- zintegrowane podejście do sytuacji konfliktowych,
- regiony jako kluczowa przestrzeń ładu,
- zapewnienie poszanowania praw człowieka, zrównoważony rozwój oraz trwały dostęp do globalnych wspólnych dóbr[593].

Komisja i Wysoki Przedstawiciel zostali wezwani do promowania[594]:

- konwencji budapeszteńskiej,
- poszanowania podstawowych praw w cyberprzestrzeni,
- wszystkich dostępnych międzynarodowych narzędzi współpracy służących przeciwdziałaniu zjawisku cyberprzestępczości,
- opracowania wspólnych komunikatów UE w sprawie cyberprzestrzeni i ścisłej współpracy z państwami członkowskimi w zakresie aspektów operacyjnych,
- pełnego wykorzystania odpowiednich instrumentów pomocy UE dla budowania potencjału technologii informacyjno-komunikacyjnych, w tym bezpieczeństwa cybernetycznego[595].

5.2
INSTRUMENTY POLITYKI CYBERBEZPIECZEŃSTWA

5.2.1. EUROPOL I SIS

Instytucją walczącą z terroryzmem w UE jest Europol odpowiedzialny za wywiad kryminalny w Europie, będący najważniejszą instytucją w tym obszarze. W 1999 r. – w wyniku nacisku ze strony Hiszpanii – zakres jego kompetencji został rozszerzony do walki z międzynarodowym terroryzmem. Jego poprzednia rola ograniczała się do gromadzenia, przekazywania i analizy danych dostarczonych przez państwowe organy policyjne i państwowe jednostki kontaktowe. Europol nie korzystał z żadnych uprawnień operacyjnych i nawet dostarczanie danych z państwowych źródeł miało tendencję do znacznie różniących się z jednego państwa członkowskiego względem drugiego. Niemniej jest to jedyna stała centralna struktura policji UE.

Zgodnie z art. 88 ust. 1 TFUE zadaniem[596] Europolu jest wspieranie i wzmacnianie działań organów policyjnych i innych organów ścigania państw unijnych oraz ich współpracy w zapobieganiu i zwalczaniu poważnej przestępczości dotykającej dwóch lub więcej państw, terroryzmu oraz form przestępczości naruszających wspólny interes objęty polityką Unii. Wszelkie działania operacyjne Europolu mają być prowadzone w powiązaniu i w porozumieniu z organami państwa członkowskiego, którego terytorium dotyczą. Stosowanie środków przymusu należy do wyłącznej kompetencji właściwych organów państwowych.

Zadaniem Europolu jest nawiązanie współpracy w zakresie zapobiegania i zwalczania międzynarodowej przestępczości zorganizowanej. Dotyczy to takich przestępstw jak:

- handel narkotykami,
- nielegalny przemyt imigrantów,
- pornografia dziecięca,

- pranie pieniędzy,
- terroryzm i cyberterroryzm[597].

Europol odpowiada również za wprowadzenie systemu komputerowego umożliwiającego udostępnianie i analizę odpowiednie danych[598].

Było to inspiracją do powstania SIS, który umożliwiał łatwość przekraczania granic obywatelom UE, prowadząc jednocześnie kontrolę i ewidencję osób z państw trzecich[599]. Podstawę prawną powołania SIS II stanowią Rozporządzenie Rady (WE) nr 2424/2001 z dnia 6 grudnia 2001 r.[600] w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz decyzja Rady z dnia 6 grudnia 2001 r. w sprawie rozwoju Sytemu Informacyjnego Schengen drugiej generacji[601]. W preambułach tych aktów podkreślono, że podstawę prawną powołania SIS II niezbędną do finansowania rozwoju tego programu z budżetu Unii Europejskiej stanowią dwa odrębne instrumenty. Nie narusza to zasady, zgodnie z którą SIS II stanowi zintegrowany system. Na mocy Rozporządzenia nr 2424/2001 i decyzji 2001/886/WSiSW System Informacyjny Schengen (SIS I), ustanowiony na podstawie tyt. IV KWS, zostaje zastąpiony Systemem Informacyjnym Schengen II (SIS II), który umożliwia włączenie do niego nowych państw członkowskich. Wspomniane akty prawne określają również procedury tworzenia i rozwoju SIS II. Rozporządzenie nr 2424/2001 oraz decyzja 2001/886/WSiSW miały obowiązywać do 31 grudnia 2006 r., okazało się jednak, że proces opracowywania SIS II będzie trwał dłużej, niż pierwotnie przewidywano. W związku z tym, w celu zapewnienia środków finansowych na rozwój SIS II po 31 grudnia 2006 r. powstała konieczność przedłużenia okresu obowiązywania omawianych aktów prawnych. W tym celu zostało wydane Rozporządzenie Rady (WE) nr 1988/2006 z dnia 21 grudnia 2006 r.[602], zmieniające wcześniejsze rozporządzenie nr 2424/2001 w sprawie rozwoju SIS II, oraz decyzja Rady z dnia 21 grudnia 2006 r.[603] zmieniająca decyzję 2001/886/WSIW w sprawie SIS II.

Szczegółowe postanowienia dotyczące utworzenia, funkcjonowania i użytkowania SIS II zawierają Rozporządzenie Parlamentu Europejskiego i Rady nr 1987/2006 z dnia 20 grudnia 2006 r.[604], decyzja Rady w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji[605], a także Rozporządzenie Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie dostępu służb odpowiedzialnych w państwach członkowskich za wydawanie świadectw rejestracji pojazdów do SIS II. Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1987/2006 stanowi niezbędną podstawę prawną systemu SIS II w kwestiach objętych zakresem stosowania TWE. Dokument Rady nr 14914/06[606] stanowi natomiast niezbędną podstawę prawną systemu SIS II w kwestiach objętych zakresem stosowania Traktatu o Unii Europejskiej.

Z kolei SIS II i VIS są instrumentami dawnego pierwszego filaru, ustanowionego na podstawie tyt. IV TWE. Przyjęto również decyzję Rady 2007/533/WSiSW i decyzję Rady (WE) nr 2008/633/WSiSW na podstawie tyt. VI TUE, które zawierają odniesienie do organu zarządzającego w kontekście zarządzania operacyjnego i oceny. Dotyczą także dostępu wyznaczonych organów państw członkowskich i Europolu do VIS na potrzeby jego przeglądania w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania. W decyzji tej powierzono organowi zarządzającemu, o którym mowa w rozporządzeniu VIS, określone zadania w zakresie monitorowania i oceny. Niezbędne zatem było przyjęcie instrumentu prawnego w ramach dawnego III filaru powierzającego agencji te zadania.

System Informacyjny Schengen ustanowiono w celu zacieśnienia współpracy między organami celnymi i policyjnymi dla zachowania porządku publicznego oraz bezpieczeństwa publicznego, w tym bezpieczeństwa narodowego. SIS stanowi instrument mający zrekompensować zniesienie kontroli na granicach wewnętrznych między państwami uczestniczącymi w tym systemie przez lepsze zabezpieczenie zewnętrznych granic Unii. System Informacyjny

Schengen drugiej generacji zastąpił SIS pierwszej generacji uruchomiony w 1995 r.

Wizowy System Informacyjny (VIS) został ustanowiony jako system wymiany informacji wizowych między państwami członkowskimi. Zgodnie z rozporządzeniem w sprawie VIS umożliwi on konsulatom i innym właściwym organom państw członkowskich wymianę informacji wizowych w celu ułatwienia identyfikacji obywateli państw trzecich, usprawnienia procedury rozpatrywania wniosków wizowych, zapobiegania zjawisku wykorzystywania różnic w przepisach prawa wizowego, ułatwienia walki z oszustwami, usprawnienia kontroli na przejściach na granicach zewnętrznych oraz na terytorium państw członkowskich, ułatwienia stosowania rozporządzenia dublińskiego oraz przyczynienia się do zapobiegania zagrożeniom bezpieczeństwa wewnętrznego państw członkowskich. Systemy państwowe podłączone do VIS miały zostać stworzone lub dostosowane i być obsługiwane przez poszczególne państwa członkowskie.

Decyzja Rady 2008/633/WSiSW[607] uzupełnia rozporządzenie w sprawie VIS w zakresie dotyczącym dostępu do jego zasobów przez wyznaczone organa państw członkowskich i Europolu w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania. Poszerza definicję przestępstw terrorystycznych zapisaną w decyzji ramowej z 13 czerwca 2002 r.[608] Ustanawia także definicję „poważnych przestępstw", które oznaczają formy przestępczości odpowiadające przestępstwom, o których mowa w art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW[609], lub są im równoważne. Państwa członkowskie wyznaczają organy upoważnione do dostępu do danych zgromadzonych w VIS zgodnie z niniejszą decyzją. Określa ona także zasady dostępu do VIS przez Europol i Eurojust, które otrzymały prawo wglądu w dane wprowadzone do SIS II oraz przeszukiwania tych danych, a także status obserwatorów podczas posiedzeń zarządu, których porządek obejmuje kwestię odnoszącą się do stosowania decyzji 2007/533/WSiSW[610]. Ponadto Europol uzyskał status obserwatora VIS podczas posiedzeń zarządu, których

porządek obejmuje kwestię odnoszącą się do stosowania decyzji 2007/633/WSiSW. Roszczenia o odszkodowanie wobec państwa członkowskiego, o których mowa w ust. 1 i ust. 2, podlegają przepisom prawa państwowego państwa członkowskiego, przeciwko któremu są skierowane, a nie przepisom wspólnotowym.

Decyzja respektuje zasadę pomocniczości, ponieważ cel proponowanych działań, czyli powierzenie agencji zarządzania operacyjnego centralnym SIS II, centralnym VIS oraz zarządzania interfejsami państwowymi, jak również częściami infrastruktury komunikacyjnej, nie może zostać osiągnięty indywidualnie przez państwa członkowskie. Decyzja nie wykracza poza to, co jest konieczne do osiągnięcia określonych w niej celów. Jest ona zgodna z zasadą proporcjonalności, gdyż zakres działalności agencji został ograniczony do minimum niezbędnego do realizacji zadań wyznaczonych dla organu zarządzającego. Działalność organu zarządzającego ogranicza się do zarządzania operacyjnego centralnym SIS II i centralnym VIS oraz interfejsami państwowymi, a także częściami infrastruktury komunikacyjnej, państwa członkowskie natomiast odpowiadają za swoje systemy wewnętrzne[611].

W kolejnym okresie sprawozdawczym przewidziano trzy główne obszary działań SIS:

- cykle testowania i związane z nimi usuwanie błędów w związku z przygotowaniami do testu drugiej fazy kluczowej i testu kompleksowego w 2012 r.,
- kontynuowanie pracy nad kwestiami bezpieczeństwa, która doprowadzi do przeprowadzenia audytu bezpieczeństwa w drugim i trzecim kwartale 2012 r.,
- testy konwertera poprzedzające pierwszą próbną migrację z SIS I do SIS II w drugim kwartale 2012 r., próbę ogólną w drugim i trzecim kwartale 2012 r. i właściwą migrację danych do SIS II przed uruchomieniem w 2013 r.

Prowadzono też prace mające na celu zapewnienie zgodności systemu z wymaganiami audytu bezpieczeństwa. Kontynuowano również przygotowania do migracji z SIS I do SIS II, wraz z

intensywnymi testami konwertera, które powinny umożliwić przeprowadzenie całego procesu przy wymaganym poziomie bezpieczeństwa[612].

Na podstawie propozycji Portugalii powstała tzw. koncepcja SISone4ALL mająca na celu podłączenie nowych państw członkowskich do aktualnie funkcjonującego SIS. Opierała się ona na założeniu, że nowe państwa członkowskie zostaną podłączone do systemu centralnego SIS do końca sierpnia 2007 r. za pomocą państwowych komponentów SIS, stworzonych na podstawie modelu systemu funkcjonującego w Portugalii. Należy podkreślić, że SISone4ALL była rozwiązaniem tymczasowym, umożliwiającym włączenie do aktualnie funkcjonującego SIS docelowo wszystkich państw członkowskich, mających obowiązek wprowadzić SIS II[613].

5.2.2. EUROJUST

Najważniejszą strukturą w dziedzinie współpracy sądowej jest transgraniczna agencja ścigania Eurojust, której powołanie zaproponowano podczas spotkania Rady Europejskiej w Tampere[614], 15–16 października 1999 r., poświęconego współpracy w zakresie wymiaru sprawiedliwości i spraw wewnętrznych Unii[615]. Eurojust miał stać się europejskim organem współpracy do walki z międzynarodową przestępczością zorganizowaną. Po przyjęciu decyzji Rady 28 lutego 2002 r. Eurojust pod wieloma względami okazał się sądowym odpowiednikiem Europolu. 6 marca 2002 r. rozpoczął formalnie swoją działalność Europejski Zespół Współpracy Sądowej na podstawie decyzji Rady UE nr 2002/187/JHA[616], zmienionej decyzją Rady 2003/659/ WSiSW z dnia 18 czerwca 2003 r.[617] Jednocześnie zaprzestała działalności tymczasowa jednostka współpracy sądowej (Pro-Eurojust); 9 czerwca 2004 r. Eurojust i Europol podpisały umowę o ścisłej współpracy.

Eurojust ułatwia współdziałanie organów ścigania poszczególnych państw, w tym przyspieszenie pomocy prawnej i ekstradycji, wsparcie dla koordynacji równoległych działań prokuratury w kilku państwach członkowskich i wymianę informacji. Nie korzysta z

żadnych uprawnień operacyjnych. Otrzymał jednak szerokie uprawnienia obejmujące transgraniczne przestępstwa, w tym terroryzm. Może więc zwracać się do właściwego organu państwa członkowskiego, aby rozważył rozpoczęcie dochodzenia lub ścigania za określone akty bądź utworzenia wspólnych zespołów dochodzeniowo-śledczych.

Pozycja Eurojustu zmieniała się po szczycie w Nicei. Traktat wprowadził do art. 29 TUE poprawkę, rozszerzając jego kompetencje jako organu umożliwiającego bliższą współpracę między organami sądowymi a innymi kompetentnymi władzami w państwach członkowskich[618]. Najistotniejsza zmiana uzgodniona w Nicei dotyczyła wspierania Eurojustu w przypadku poważnych przestępstw transgranicznych oraz ułatwienia ścisłej współpracy między Eurojustem a Europejską Siecią Sądową, w szczególności w celu realizacji wniosków o ekstradycję.

Zgodnie z art. 3 decyzji Rady do zadań Eurojustu należy:

- stymulowanie i poprawa koordynacji między właściwymi władzami państw członkowskich, dochodzenie i ściganie w państwach członkowskich uwzględniające wszelkie wnioski składane przez właściwe władze państwa członkowskiego i wszelkie informacje dostarczone przez organy właściwe na podstawie przepisów przyjętych w ramach traktatów,
- poprawa współpracy między właściwymi władzami państw członkowskich, w szczególności ułatwianie realizacji wniosków i decyzji dotyczących współpracy sądowej, w tym również jeżeli chodzi o instrumenty służące wdrożeniu zasady wzajemnego uznawania,
- wspieranie właściwych władz państw członkowskich w celu usprawnienia ich dochodzenia i ścigania.

Zgodnie z zasadami przewidzianymi decyzją Rady i na wniosek właściwych władz państwa członkowskiego Eurojust może także wspomagać postępowanie przygotowawcze i ściganie dotyczące tylko tego państwa członkowskiego oraz państwa nieczłonkowskiego, jeśli została zawarta umowa ustanawiająca współpracę z odnośnym

państwem lub jeśli w szczególnym przypadku istnieją szczególne powody do udzielenia pomocy[619].

W celu realizacji swoich zadań Eurojust działa przez jednego lub więcej odpowiednich przedstawicieli państwowych lub jako Kolegium. Współpracuje z Europolem, co wynika z art. 26 ust. 1 decyzji. Posiada również osobowość prawną, a kontrolę nad ogólną działalnością Eurojustu w zakresie gromadzenia, przetwarzania i dysponowania danymi sprawuje Wspólny Organ Nadzorczy[620].

Ze względu na stałość oraz skład (każde państwo członkowskie ma wyznaczonego spośród swoich władz sądowych przedstawiciela) Eurojust ułatwia koordynację spraw wielostronnej współpracy sądowej. Jest to szczególnie przydatne w walce z terroryzmem. To jedyna dziedzina, w której Rada wyznaczyła szczegółowe obowiązki państw członkowskich w zakresie systematycznego przekazywania informacji do Eurojustu. Instrument mający na celu wzmocnienie Eurojustu jest obecnie przedmiotem dyskusji w Radzie UE[621].

5.2.3. AGENCJA UE DS. CYBERBEZPIECZEŃSTWA (EUROPEJSKA AGENCJA DS. BEZPIECZEŃSTWA SIECI I INFORMACJI)

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji[622], powołana 10 marca 2004 r., jest ośrodkiem ekspertyzy w zakresie zagadnień związanych z bezpieczeństwem internetowym, który ma za zadanie zapewnienie pomocy władzom państw członkowskich.

Według rozporządzenia powołującego Agencję powinna ona wykonywać swoje zadania przy pełnej współpracy z państwami członkowskimi, a także być otwarta na kontakty z przedstawicielami biznesu, przemysłu i innymi udziałowcami. Ponieważ sieci elektroniczne stanowią w dużym stopniu własność prywatną, Agencja opiera się na danych wejściowych pochodzących z sektora prywatnego oraz współpracy z tym sektorem. Do jej zadań należy m.in. zbieranie stosownych informacji w celu przeanalizowania ryzyka bieżącego i powstającego (szczególnie w Europie), które może wpływać na dostępność i elastyczność sieci łączności elektronicznej oraz autentyczność, integralność i poufność informacji

udostępnianych i przesyłanych za pomocą sieci, a także dostarczanie wyników analiz państwom członkowskim i Komisji. Ponadto ma się zajmować doradztwem[96], oferować na żądanie pomoc w ramach swoich kompetencji, rozszerzać współpracę między różnymi instytucjami działającymi w obszarze bezpieczeństwa sieci i informacji, m.in. poprzez organizowanie regularnych konsultacji z przemysłem, uniwersytetami i innymi stosownymi sektorami oraz tworzenie sieci kontaktów dla organów Wspólnoty, organów sektora publicznego, wyznaczonych przez państwa członkowskie, sektora prywatnego oraz organów konsumenckich.

Ponadto do obowiązków Agencji należy:

- ułatwianie współpracy Komisji z państwami członkowskimi w zakresie rozwoju wspólnych metodologii w celu ochrony, określania i reagowania na problemy dotyczące bezpieczeństwa sieci i informacji;
- przyczynianie się do wzrostu świadomości i dostępności aktualnych, celowych i wszechstronnych informacji na temat bezpieczeństwa sieci i informacji w stosunku do wszystkich użytkowników, m.in. poprzez promowanie wymiany najlepszych praktyk (w postaci doradztwa, szkoleń i kursów), w tym metod ostrzegania użytkowników oraz poszukiwanie współdziałania między inicjatywami w sektorach publicznym i prywatnym;
- wspieranie Komisji i państw członkowskich w dialogu z przemysłem w celu określania problemów dotyczących bezpieczeństwa sprzętu i oprogramowania;
- śledzenie rozwoju norm w zakresie produktów i usług dotyczących bezpieczeństwa sieci i informacji;
- doradzanie Komisji w obszarze badań bezpieczeństwa sieci i informacji;
- skuteczne stosowanie technologii zapobiegających powstawaniu ryzyka, promowanie działań z zakresu oceny ryzyka, współdziałających ze sobą rozwiązań z tej dziedziny oraz badanie tego typu rozwiązań, stosowanych w organizacjach sektorów publicznego i prywatnego;

- uczestniczenie w działaniach Wspólnoty zmierzających do współpracy z krajami trzecimi, a w stosownych przypadkach z organizacjami międzynarodowymi w celu promowania wspólnej, globalnej propozycji dotyczącej bezpieczeństwa sieci i informacji i tym samym przyczynianie się do rozwoju kultury bezpieczeństwa sieci i informacji;
- wyrażanie w sposób niezależny własnych wniosków, orientacji i doradzanie w sprawach zgodnych z zakresem i celami Agencji.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r.[623] w sprawie ENISA (Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie – CA) jest drugą po dyrektywie NIS ogólnoeuropejską regulacją w dziedzinie cyberbezpieczeństwa.

CA składa się z dwóch części. Pierwszą stanowi nowy permanentny mandat dla ENISA, której nazwa została zmieniona z Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji na Agencję UE ds. Cyberbezpieczeństwa. Rola ENISA została znacznie wzmocniona nie tylko przez ciągły mandat, ale także przez wiele nowych obowiązków związanych z wejściem w życie Dyrektywy NIS oraz europejskich ram certyfikacji. Podstawowym zadaniem jest wspieranie spójnego wprowadzania odpowiednich ram prawnych w celu skutecznego wdrożenia dyrektywy (UE) 2016/1148 i innych stosownych instrumentów prawnych zawierających aspekty dotyczące cyberbezpieczeństwa, co ma mieć kluczowe znaczenie dla zwiększenia cyberodporności. Powinna również wspomagać UE i państwa członkowskie w opracowaniu i aktualizacji strategii w zakresie cyberbezpieczeństwa. Drugą częścią natomiast jest rozporządzenie tworzące europejskie ramy certyfikacji cyberbezpieczeństwa dla produktów i usług ICT. To bardzo istotna regulacja, która znacznie zmieni funkcjonujący obecnie model certyfikacji, zdominowany przez SOG-IS (*Senior Official Group Information Security Systems)*. Akt o cyberbezpieczeństwie wszedł w życie 27 czerwca 2019 r.

5.2.4. EUROPEJSKIE CENTRUM DS. WALKI Z CYBERPRZESTĘPCZOŚCIĄ

Europejskie Centrum ds. Walki z Cyberprzestępczością jest agencją ustanowioną przez KE w *Strategii bezpieczeństwa wewnętrznego UE w działaniu*[624,625]. Otwarcie agencji ds. walki z cyberprzestępczością miało miejsce 11 stycznia 2013 r. Europejskie Centrum ds. Walki z Cyberprzestępczością jest kontynuacją myśli ustawodawcy zawartej w dyrektywie 2011/92/UE z dnia 13 grudnia 2011 r. Centrum działa w ramach Europolu. Jego głównym zadaniem jest ochrona profili użytkowników serwisów społecznościowych przed zagrożeniami ze strony środowisk przestępczych oraz udzielanie pomocy w zwalczaniu przestępstw internetowych, które przynoszą poważne szkody ich ofiarom. Celem jego działalności jest walka z następującymi rodzajami przestępstw:

- cyberprzestępstwami popełnionymi przez zorganizowane grupy przestępcze, zwłaszcza przynoszącymi duże zyski, czyli oszustwami internetowymi;
- cyberprzestępstwami wyrządzającymi poważne szkody ofiarom, czyli przemocą seksualną wobec dzieci w cyberprzestrzeni;
- cyberprzestępstwami (również cyberatakami) przeciwko infrastrukturze krytycznej i systemom informatycznym w Unii Europejskiej.

Aby zrealizować wymienione cele, Europejskie Centrum ds. Walki z Cyberprzestępczością:

- jest centralnym ośrodkiem wymiany informacji karnych i wywiadowczych;
- wspiera państwa członkowskie w przeprowadzanych operacjach i dochodzeniach poprzez dostarczanie analiz, wiedzy i koordynację działań;
- oferuje wiele produktów do analizy działań strategicznych umożliwiających świadome podejmowanie decyzji na szczeblach taktycznym i strategicznym w zakresie zwalczania i zapobiegania cyberprzestępczości,

- buduje potencjał i przeprowadza szkolenia, zwłaszcza w odniesieniu do odpowiednich organów państw członkowskich;
- zapewnia wysoko wyspecjalizowanych specjalistów i ekspertyzy kryminalistyczne, które mogą być wykorzystane w dochodzeniach i operacjach.

1 sierpnia 2014 r. powołano w ramach EC3 kolejną grupę zadaniową ds. cyberprzestępczości o nazwie J-CAT. Ma ona za zadanie prowadzenie wywiadu, zbieranie informacji i przeprowadzanie skoordynowanych działań przeciwko cyberprzestępczości. Realizacja powyższych zadań ma nastąpić przez koordynację działań, wspólne ustalanie priorytetów, przygotowanie, wszczynanie i prowadzenie dochodzeń transgranicznych. J-CAT zajmuje się zwalczaniem cyberprzestępstw takich, jak malware, botnety, oszustwa online, pranie pieniędzy, w tym walut wirtualnych, oraz nadużyciami seksualnymi dzieci w cyberprzestrzeni[626].

5.2.5. DECYZJE RAMOWE I STRATEGIE UE DOTYCZĄCE PROBLEMATYKI ZWALCZANIA CYBERTERRORYZMU

Pierwszymi instrumentami regulującymi kwestie cyberbezpieczeństwa w Unii Europejskiej były dyrektywa 2002/58/WE z dnia 12 lipca 2002 r. o prywatności i łączności elektronicznej[627], dyrektywa 2002/22/WE w sprawie usługi powszechnej[628], dyrektywa 2002/20/WE w sprawie zezwoleń[629], decyzja ramowa 2005/222/WSiSW Rady z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[630] oraz rozporządzenie (WE) nr 460/2004 z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji[631].

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady Unii Europejskiej dotyczyła przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej. Stanowiła *lex specialis* wobec dyrektywy 95/46/WE[632]. Celem nadrzędnym

dyrektywy 2002/58/WE było zapewnienie zasad ustanowionych przez dyrektywę 95/46/WE w sektorze komunikacji elektronicznej.

Zgodnie z dyrektywą 2002/58/WE zobowiązano dostawców publicznie dostępnych usług łączności elektronicznej do podjęcia właściwych środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa oferowanych przez siebie usług. Należy zaznaczyć, że poufność nie ma jednak zastosowania w przypadku przetwarzania danych w celu udokumentowania faktu transakcji lub prowadzenia korespondencji handlowej. Zgodnie z art. 5 ust. 3 dyrektywy 2002/58/WE dozwolone jest techniczne przechowywanie danych oraz dostęp do nich w celu wykonania lub ułatwiania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej lub w sytuacji, gdy jest to konieczne, aby dostarczyć usługi społeczeństwu informacyjnemu, wyraźnie zażądanej (zamawianej) przez abonenta lub użytkownika. Istotę tego przepisu stanowi generalna dopuszczalność wykorzystywania rozwiązań technologicznych dających usługodawcy dostęp do niektórych danych użytkowników końcowych[633]. Na mocy art. 13 został zakazany spamming, zwłaszcza wysyłanie poczty elektronicznej do celów marketingu bezpośredniego, gdzie przerobiono lub ukryto tożsamość nadawcy, w którego imieniu wysłano komunikat, lub bez aktualnego adresu, na który odbiorca może wysłać wniosek o zaprzestanie wysyłania takich komunikatów[634].

Kolejne dwa instrumenty to dyrektywy 2002/22/WE i 2002/21/WE, które definiowały i regulowały zestaw usług, o którym mowa w art. 2 dyrektywy 2002/22/WE składających się na usługę powszechną, co wynika z art. 4 do 7 dyrektywy 2002/22/WE, przy czym dostęp do Internetu znalazł się już w pierwszym z tych artykułów. Zgodnie z art. 4 ust. 1 państwo członkowskie miało obowiązek zapewnić, aby co najmniej jedno przedsiębiorstwo spełniło wszelkie wnioski o stacjonarne podłączenie do publicznej sieci telefonicznej oraz o dostęp do publicznie dostępnych usług telefonicznych. W myśl ust. 2 tak zapewnione podłączenie powinno zezwalać użytkownikom końcowym na inicjowanie i otrzymywanie wywołań lokalnych, krajowych i międzynarodowych, komunikację faksową oraz

przesyłanie danych z szybkościami pozwalającymi na funkcjonalny dostęp do Internetu, biorąc pod uwagę przeważające technologie wykorzystywane przez większość abonentów oraz technologiczne możliwości zastosowań. Dyrektywę 2002/22/WE zmieniła dyrektywa 2009/136/WE, a dyrektywę 2002/21/WE zastąpiła dyrektywa 2009/140/WE z dnia 25 listopada 2009 r., przy czym dyrektywy te nie dokonały znaczących zmian w przytoczonych przepisach. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca *Europejski kodeks łączności elektronicznej*[635] zastąpiła dyrektywę 2002/20/WE, dyrektywę 2002/21/WE i dyrektywę 2002/22/WE. Tym samym, w wyniku objęcia zakresem tej dyrektywy tak wielu zagadnień, *Europejski kodeks łączności elektronicznej* stanowi akt kompleksowo regulujący rynek telekomunikacyjny. Do najważniejszych obszarów regulowanych przez ten dokument należy zaliczyć:

- status i kompetencje krajowych organów regulacyjnych oraz zasady ich współpracy z innymi właściwymi organami, w tym Organem Europejskich Regulatorów Łączności Elektronicznej (BEREC) (art. 5–11);
- kwestię ogólnych zezwoleń na sieci i usługi łączności elektronicznej, czyli m.in. zasady prowadzenia działalności telekomunikacyjnej czy prawa i obowiązki przedsiębiorców telekomunikacyjnych (art. 12–19);
- pozasądowe rozwiązywanie sporów między przedsiębiorcami a abonentami (art. 25);
- rozstrzyganie sporów między przedsiębiorstwami, w tym sporów transgranicznych (art. 26–27);
- spójne i zharmonizowane przydzielanie pasm widma radiowego oraz zasady zarządzania nimi i użytkowania ich (art. 35–37);
- bezpieczeństwo sieci i usług(art. 40–41);
- dostęp do urządzeń sieci bezprzewodowej (lokalne sieci radiowe) (art. 56–57);
- zagadnienia związane z dostępem telekomunikacyjnym i umowami międzyoperatorskimi (art. 61);

- kwestie dotyczące zasad i sposobu zapewnienia efektywnej konkurencji na rynku, procedury analizy rynku, zasad ustalenia przedsiębiorcy o znaczącej pozycji rynkowej (art. 62–83);
- nowo określone obowiązki świadczenia usługi powszechnej (art. 82–92);
- ochrona praw abonentów, w tym m.in. osób niepełnosprawnych, oraz wymogi w zakresie jasności i przejrzystości umów, dostęp do porównywarki cen, taryf oraz jakości usługi dostępu do Internetu oraz usług łączności interpersonalnej niewykorzystujących numerów, zapewnienie możliwości przenoszenia usług dostępu do Internetu przez użytkowników końcowych w sposób podobny do przenoszenia numeru telefonu (art. 98–108).

Ponadto jako pierwsza dyrektywa unijna rozszerza ona wprost regulację telekomunikacyjną na usługi *over-the-top*. W tym celu zakresem definicji „usługi łączności elektronicznej" objęto usługi łączności interpersonalnej umożliwiające bezpośrednią wymianę informacji między określoną liczbą osób, np. Skype lub Facebook, przy czym dyrektywa rozróżnia usługi łączności interpersonalnej wykorzystujące numery (np. połączenia Skype na telefon) i niewykorzystujące numerów (np. połączenia za pośrednictwem Facebooka). Obowiązki tych pierwszych zrównają się z obowiązkami „tradycyjnych" operatorów telekomunikacyjnych, co na gruncie poprzednich dyrektyw było sporne. W przypadku dostawców usług niewykorzystujących numerów zastosowanie znajdzie jedynie część przepisów, w tym związanych z bezpieczeństwem sieci lub przekazywaniem informacji krajowemu organowi regulacyjnemu.

W celu zapewnienia wysokiego i skutecznego poziomu bezpieczeństwa sieci i informacji we Wspólnocie oraz rozwijania kultury bezpieczeństwa sieci i informacji na rzecz obywateli, konsumentów, przedsiębiorstw oraz organizacji sektora publicznego Unii Europejskiej, a zatem zapewnienia płynnego funkcjonowania rynku wewnętrznego, 10 marca 2004 r. ustanowiono Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji[636]. Agencja ma stać się

ośrodkiem ekspertyzy ds. zagadnień związanych z bezpieczeństwem internetowym[637].

Kolejnym instrumentem była dyrektywa 2005/222/WSiSW w sprawie ataków na systemy informatyczne. Jej celem było „usprawnienie współpracy między organami sądowymi i innymi właściwymi organami, włącznie z policją i innymi wyspecjalizowanymi organami ścigania państw członkowskich UE, przez zbliżanie zasad prawa karnego w państwach członkowskich w dziedzinie ataków na systemy informatyczne". Decyzja ramowa po raz pierwszy określiła też jako niezbędną konieczność wprowadzenia sankcji karnych za ataki na systemy informatyczne. Decyzja ramowa Rady 2005/222/WSiSW została zastąpiona dyrektywą Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r., dotyczącą ataków na systemy informatyczne i uchylającą poprzednią decyzję ramową Rady.

8 grudnia 2008 r. została przyjęta dyrektywa w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy[638]. Z kolei dyrektywa 2013/40/UE[639] z dnia 12 sierpnia 2013 r. zastąpiła dotyczącą tej samej problematyki wcześniejszą decyzję ramową Rady 2005/222/WSiSW[640] z dnia 24 lutego 2005 r. i stanowi jej rozwinięcie oraz uszczegółowienie. Celem dyrektywy jest usprawnienie współpracy właściwych organów państw członkowskich w dziedzinie ataków na systemy informatyczne oraz ustanowienie minimalnych norm dotyczących określania przestępstw i kar w dziedzinie ataków na systemy informatyczne. Zgodnie z art. 2 dyrektywy w sprawie ataków na systemy informatyczne „system informatyczny" oznacza wszelkie urządzenia lub grupę podłączonych lub powiązanych urządzeń, z których jedno lub więcej dokonuje automatycznego przetwarzania danych komputerowych, a także danych przechowywanych, przetwarzanych, odzyskiwanych lub przekazanych przez nie w celach ich eksploatacji, użycia, ochrony lub utrzymania. „Dane komputerowe" oznaczają natomiast wszelkie przedstawienie faktów, informacji lub koncepcji w formie odpowiedniej do przetwarzania w systemie informatycznym, włącznie z programem odpowiednim do

spowodowania wykonania funkcji przez system. Terminem „bezprawne” określono dostęp lub ingerencję, na którą właściciel, inny posiadacz prawa do systemu lub jego części nie udzielił zgody lub która nie jest dozwolona na mocy prawa państwowego[641].

W celu zbliżenia porządków prawnych uznano, że w każdym państwie członkowskim karany powinien być nielegalny dostęp do systemu informatycznego oraz nielegalna ingerencja w system i dane. Nielegalny dostęp do systemu informatycznego rozumiany jest jako umyślny, bezprawny dostęp do całości lub części systemu informatycznego[642]. Państwa członkowskie mogą swobodnie decydować, czy jest on objęty oskarżeniem zawsze, czy też jedynie w sytuacji, gdy przestępstwo jest popełniane z naruszeniem zabezpieczenia. Nielegalna ingerencja w system w myśl art. 4 dyrektywy to bezprawne, umyślne, poważne naruszenie lub przerwanie funkcjonowania systemu informatycznego przez wprowadzanie, przekazywanie, uszkadzanie, usuwanie, niszczenie, zmienianie, zatajanie lub uczynienie niedostępnymi danych komputerowych. Z kolei nielegalna ingerencja w dane zgodnie z art. 5 dyrektywy oznacza umyślne i bezprawne usunięcie, uszkodzenie, pogorszenie, zmianę, zatajanie lub uczynienie niedostępnymi danych komputerowych w systemie informatycznym[643].

W ustawodawstwie Unii Europejskiej zapisano regulacje odnoszące się do kryminalizacji działań mających na celu rozpowszechnianie informacji zakazanych przez prawo, także za pośrednictwem sieci komputerowych. Dyrektywa nr 2011/93/UE z 13 grudnia 2011 r.[644] zawiera przepisy dotyczące zwalczania wykorzystywania seksualnego dzieci, w tym pornografii dziecięcej rozpowszechnianej za pośrednictwem Internetu. Ustanawia a minimalne normy dotyczące określania przestępstw i kar dotyczących niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci, pornografii dziecięcej oraz nagabywania dzieci dla celów seksualnych. Wprowadza ona również przepisy służące lepszemu zapobieganiu takim przestępstwom i lepszej ochronie pokrzywdzonych w ich wyniku (art. 1 dyrektywy). W art. 5 dyrektywy znalazły się postanowienia dotyczące

przestępstw związanych z pornografią dziecięcą. Podobnie jak dyrektywa Rady Europy z 2007 r. zalecają one kryminalizację określonych przestępstw, wskazując jednocześnie minimalne ustawowe sankcje za ich popełnienie. W art. 5 ust. 3 przewidziano kryminalizację świadomego uzyskiwania dostępu za pośrednictwem technologii informacyjno-komunikacyjnych do pornografii dziecięcej, przy czym czyn ten powinien być opatrzony sankcją karną w maksymalnym wymiarze co najmniej roku pozbawienia wolności.

Dyrektywa 2008/114/WE w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony[645] wprowadziła po raz pierwszy do porządku prawnego Unii Europejskiej definicje infrastruktury krytycznej, europejskiej infrastruktury krytycznej (EIK), ochrony infrastruktury krytycznej oraz pojęcie właściciela (operatora) europejskiej infrastruktury krytycznej. W dokumencie określono sposób rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej, a także obowiązki państw członkowskich tej infrastruktury. Zgodnie z art. 1 dyrektywy infrastruktura krytyczna oznacza składnik, system lub część infrastruktury zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji.

System jest oparty na sieci S-TESTA, co dawało możliwość przetwarzania informacji oznaczonych klauzulą tajności RESTREINT UE. Prace nad stworzeniem systemu powierzono firmie Unisys. W ramach prac w grupie roboczej Rady UE ds. ochrony ludności (PROCIV), która była odpowiedzialna za procedowanie przedstawionego projektu decyzji, postanowiono, że nie ma potrzeby tworzenia systemu wymiany informacji o zagrożeniach, gdyż byłoby to bardzo kosztowne. Jednocześnie wskazano na istnienie innych kanałów, którymi tego typu informacje mogły być przekazywane zarówno między stolicami państw członkowskich, jak i Brukselą. Wiele państw postulowało również, że nie widzi możliwości

umieszczania materiałów niejawnych na platformie i chce, aby udział w niej był całkowicie dobrowolny. W wyniku konsultacji postanowiono, że prace nad projektem zostaną wstrzymane do czasu przedstawienia przez wykonawcę prototypu, który pozwoli krajom na zapoznanie się z jego funkcjonalnością W związku z tym powstał dobrowolny system pozwalający na wymianę informacji i materiałów na temat stosowania najlepszych praktyk z zakresu ochrony infrastruktury krytycznej między państwami UE a Komisją. Jego podstawą jest strona internetowa dostępna tylko dla posiadaczy hasła. Nie jest możliwe umieszczanie na niej materiałów niejawnych.

14 lutego 2013 r. Komisja Europejska przedstawiła wraz z Wysokim Przedstawicielem Unii ds. Zagranicznych i Polityki Bezpieczeństwa komunikat w sprawie europejskiej strategii bezpieczeństwa cybernetycznego *Otwarta, bezpieczna i chroniona cyberprzestrzeń*”[646]. Strategii towarzyszył wniosek legislacyjny w sprawie dyrektywy dotyczącej cyberbezpieczeństwa.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[647] została przyjęta dnia 6 lipca 2016 r. (zwana dalej dyrektywą 2016/1148 lub NIS). Zobowiązuje ona wszystkie państwa członkowskie UE do zagwarantowania minimalnego poziomu zdolności krajowych w dziedzinie cyberbezpieczeństwa przez ustanowienie organów właściwych oraz pojedynczego punktu kontaktowego ds. cyberbezpieczeństwa, powołanie zespołów reagowania na incydenty komputerowe (CSIRT) oraz przyjęcia krajowych strategii w zakresie cyberbezpieczeństwa.

Dyrektywa formułuje obowiązki służące zapewnieniu cyberbezpieczeństwa systemów informacyjnych w sektorach usług mających kluczowe znaczenie dla utrzymania krytycznej działalności społeczno-gospodarczej, czyli w energetyce, transporcie, bankowości, instytucjach finansowych, sektorze ochrony zdrowia, zaopatrzenia w wodę i infrastrukturze cyfrowej[648]. Wprowadza pojęcie operatora usługi kluczowej, czyli podmiotu świadczącego z wykorzystaniem systemów informacyjnych usługę kluczową, w

której przypadku incydenty bezpieczeństwa teleinformatycznego mogłyby mieć istotny wpływ na jej świadczenie.

Dyrektywa 2016/1148 jest pierwszym aktem prawa UE w zakresie cyberbezpieczeństwa wprowadzającym regulacje międzysektorowe. Koncentruje się wokół trzech filarów:

- instytucji, które powinny powstać we wszystkich państwach członkowskich,
- współpracy na poziomie europejskim,
- zobowiązań w zakresie bezpieczeństwa sieci i informacji.

W zakresie filaru pierwszego każde państwo członkowskie jest zobligowane do ustanowienia organów właściwych ds. bezpieczeństwa sieci i informacji, odpowiedzialnych za monitorowanie stosowania jej przepisów w sektorach objętych jej zakresem. Ze względu na różnice w krajowych strukturach zarządzania państwa członkowskie mogą wyznaczać więcej niż jeden właściwy organ krajowy odpowiedzialny za wykonywanie zadań związanych z cyberbezpieczeństwem operatorów usług kluczowych i dostawców usług cyfrowych.

Drugi filar dyrektywy obejmuje współpracę między państwami członkowskimi. Dyrektywa 2016/1148 wprowadza mechanizmy współpracy na dwóch poziomach: technicznym i polityczno-strategicznym. Współpraca techniczna ma być zapewniona przez europejską sieć CISRT oraz stworzenie mechanizmów wymiany informacji o incydentach transgranicznych między CSIRT wyznaczonymi dla operatorów usług kluczowych oraz dostawcami usług cyfrowych. Współpraca na poziomie polityczno-strategicznym natomiast ma być realizowana przez utworzenie Grupy Współpracy, która zajmie się wypracowaniem wspólnych koncepcji strategicznych i będzie przyjmowała m.in. roczne raporty od właściwych organów.

Trzecim filarem dyrektywy są zobowiązania w zakresie bezpieczeństwa sieci i informacji, które są różne w zależności od załącznika. Operatorzy usług kluczowych zostaną zobowiązani do dokonania oceny zagrożeń cyberbezpieczeństwa, na jakie są narażeni, oraz do przyjęcia odpowiednich i proporcjonalnych

środków mających na celu zapewnienie bezpieczeństwa sieci i informacji. Podmioty te będą zgłaszać właściwym organom wszelkich incydentów poważnie zagrażających ich sieciom i systemom informatycznym, mogących znacząco zakłócić ciągłość działania kluczowych usług (obowiązkowe raportowanie). Raportowaniu będą podlegać incydenty o „znaczącym wpływie na ciągłość działania operatorów", co *de facto* oznacza, że progi raportowania określą państwa członkowskie w procesie implementacji. Podmioty załącznika III zostaną objęte regulacją reaktywnym nadzorem *ex post*.

Dyrektywa nakłada na państwa członkowskie obowiązek przyjęcia narodowej strategii bezpieczeństwa sieci i informacji, w której zostaną określone m.in. narodowe cele i priorytety w dziedzinie cyberbezpieczeństwa, role i obowiązki organów administracji publicznej w procesie osiągania wyznaczonych celów, zasady współpracy sektorów publicznego i prywatnego oraz krajowa analiza ryzyka i zadania w zakresie edukacji na rzecz cyberbezpieczeństwa. Przepisy umożliwiają zarówno stworzenie scentralizowanego systemu na poziomie krajowym, jak i podzielenie kompetencji między różne podmioty wymieniające informacje za pomocą opracowanych mechanizmów współpracy. Ponadto dyrektywa zobowiązuje wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu krajowych zdolności w dziedzinie bezpieczeństwa teleinformatycznego i daje organom publicznym konkretne narzędzie do przeciwdziałania oraz reakcji na incydenty w cyberprzestrzeni. Będzie to możliwe m.in. dzięki nałożonym obowiązkom raportowania, przygotowania krajowych strategii, skoordynowaniu przepływu informacji oraz zinstytucjonalizowaniu współpracy CSIRT.

Każde państwo członkowskie, w przypadku ustanowienia wielu organów właściwych, musi ustanowić Pojedynczy Punkt Kontaktowy (PPK). Jego zadaniem ma być wzmacnianie współpracy między państwami członkowskimi. Ponadto będzie gromadził informacje o incydentach w skali kraju i przez kontakt ze swoimi odpowiednikami z zagranicy wzmacniał wymianę informacji o znaczących, transnarodowych incydentach.

Ostatnią wymaganą przez dyrektywę instytucją jest CSIRT, obejmujący cały zakres podmiotowy regulacji. Państwa członkowskie mogą wskazać kilka CSIRT, mogą także wskazać jeden, np. w obrębie organu właściwego. Dyrektywa zachowuje dużą elastyczność, jeżeli chodzi o wewnętrzne struktury systemu cyberbezpieczeństwa. Oznacza to, że kraje członkowskie mogą wyznaczyć jeden CSIRT narodowy dla całego kraju, kilka CSIRT poziomu narodowego bądź zbudować sieć CSIRT sektorowych.

Najważniejsze jest jednak to, że dyrektywa 2016/1148 stanowi harmonizację minimalną i nie ogranicza możliwości państw członkowskich do regulowania problematyki bezpieczeństwa teleinformatycznego administracji publicznej, a także objęcia zakresem w większej liczby podmiotów. Wszystko to zależy od państw członkowskich.

Nie należy zapominać o pierwszej europejskiej strategii bezpieczeństwa z 2003 r. oraz strategii UE w dziedzinie walki z terroryzmem z 2005 r. uważanej za krok milowy w zakresie polityki bezpieczeństwa Unii, ponieważ po raz pierwszy państwa europejskie zdecydowały się zdefiniować potencjalne zagrożenia i określiły działania mogące przeciwdziałać ich powstaniu. Jako główne zagrożenia bezpieczeństwa strategia wymienia terroryzm we wszystkich jego odmianach.

To dzięki ESB z 2003 r. Parlament Europejski wraz z Radą Unii Europejskiej powołały pierwszy wspólnotowy wyspecjalizowany organ mający na celu ochronę cyberprzestrzeni i zwalczania zagrożeń cybernetycznych – Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (European Network and Information Security Agency – ENISA).

Strategia z 2005 r. kładła główny nacisk na zwalczanie terroryzmu w skali światowej, przestrzegając praw człowieka, aby Europa była obszarem wolności, bezpieczeństwa i sprawiedliwości dla swoich obywateli. Podstawowym założeniem strategii UE jest przekonanie, że bezpośrednia odpowiedzialność za skuteczność działań ochronnych przeciwko zagrożeniom terroryzmu i cyberterroryzmu spoczywa na państwach członkowskich, nie zaś na Unii jako organizacji państw. Nie oznacza to jednak, że UE nie ma odgrywać

żadnej roli w tym procesie, ma ona jednak przybierać następujące formy:

- ułatwiania współpracy europejskiej, tj. współpracy w dziedzinie bezpiecznej wymiany informacji między państwami członkowskimi a instytucjami, w tym między policją a sądownictwem;
- budowy zbiorowego potencjału, tj. zapewnienie na szczeblu UE zdolności do rozumienia zagrożenia terroryzmem i zapewnienia wspólnych reakcji politycznych, optymalne wykorzystanie możliwości organów europejskich, jak Europol, Eurojust, Frontex;
- wspierania partnerstwa międzynarodowego, tj. współpraca z podmiotami spoza UE – zwłaszcza z ONZ na rzecz walki z terroryzmem.

Strategia Cyberbezpieczeństwa dla UE z 2013 r. była kolejnym milowym krokiem w zakresie ochrony cyberprzestrzeni w państwach UE. Z dzisiejszej perspektywy można stwierdzić, że przyjęto ją zbyt późno w stosunku do rzeczywistych potrzeb i zagrożeń. Wyróżniono w niej pięć strategicznych priorytetów z zakresu cyberbezpieczeństwa:

- osiągnięcie odporności na cyberzagrożenia,
- radykalne ograniczenie cyberprzestępczości,
- opracowanie polityki obronnej i rozbudowa zdolności w dziedzinie cyberbezpieczeństwa w powiązaniu ze Wspólną Polityką Bezpieczeństwa i Obrony,
- rozbudowa zasobów przemysłowych i technologicznych,
- ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE.

Globalna strategia UE na rzecz polityki zagranicznej i bezpieczeństwa została przyjęta przez Radę Europejską 28 czerwca 2016 r.[649] Określa ona wspólne interesy UE i państw członkowskich. Jej główne cele to: bezpieczeństwo obywateli i terytorium, dobrobyt, demokracja i ład

światowy, które mają doprowadzić do stworzenia wiarygodnej, reaktywnej i spójnej Unii Europejskiej.

Zasady, którymi zaczęła kierować się Unia Europejska, to: jedność, współdziałanie z innymi państwami, odpowiedzialność, pogłębianie partnerstw zewnętrznych.

Nowy dokument po raz pierwszy wyraził potrzebę „utrzymania i rozwoju przez UE podstawowych zdolności do zapewnienia bezpieczeństwa gospodarki cyfrowej, społeczeństwa i demokracji". Celem polityki UE stało się zmniejszenie fragmentaryzacji rynku, a także rozwinięcie zdolności gospodarczych i poprawa działań wobec incydentów cybernetycznych. Konkretne działania polityczne nastąpiły w 2017 r. Jednym z zadań polityki UE w zakresie cyberbezpieczeństwa stało się wzmocnienie zdolności i współpracy dotyczących bezpieczeństwa cybernetycznego w celu zapewnienia takiego samego poziomu rozwoju we wszystkich państwach członkowskich. W tym celu Parlament Europejski i Rada UE wprowadziły w 2016 r. dwa akty prawne, które obecnie kształtują podstawowe ramy europejskiego bezpieczeństwa cybernetycznego w wymiarze społeczno-gospodarczym.

We wrześniu 2017 r. Komisja Europejska rozpoczęła przegląd *Europejskiej strategii bezpieczeństwa cybernetycznego* z 2013 r., wydając dokument roboczy przedstawiający jej ocenę[650]. Zgodnie z nią wspomniana strategia była tylko częściowo skuteczna z powodu niewystarczających zasobów i ograniczonego zaangażowania kluczowych podmiotów. Ponadto od tamtej pory możliwości i zagrożenia w cyberprzestrzeni znacznie się rozwinęły. Czynniki te uzasadniły więc podjęcie ważnego kroku, tj. odnowienia strategii cyberbezpieczeństwa.

Podstawą reformy miały być działania przewidziane w strategii cyberbezpieczeństwa oraz główny jej filar – dyrektywa o bezpieczeństwie sieci i informacji (dyrektywa NIS)[651], która ma na celu zapewnienie sprawnego funkcjonowania europejskiego rynku wewnętrznego. Wymaga ona także, aby wszystkie państwa UE posiadały zdolności w zakresie cyberbezpieczeństwa oraz by współpracowały ze sobą na poziomie strategicznym i operacyjnym.

Drugim aktem prawnym jest GDPR[652], które dotyczy danych osobowych obywateli UE. Celem tego rozporządzenia jest ochrona praw jednostki w związku z przetwarzaniem danych osobowych. Przepisy określają prawo dostępu do informacji oraz regulują gromadzenie, przetwarzanie i przekazywanie danych między podmiotami publicznymi[653]. W wyniku ogromnej skali cyberzagrożeń coraz częściej zaczęły pojawiać się głosy, że UE nie spełnia oczekiwań w dziedzinie cyberobrony[654]. Ponadto państwa członkowskie opracowywały rozbieżne strategie cyberbezpieczeństwa, wyrażały odmienne poglądy na temat tego, jak podmioty państwowe oraz instytucje UE powinny przyczyniać się do odporności cybernetycznej na szczeblu europejskim. W efekcie każdy obszar *Europejskiej strategii bezpieczeństwa cybernetycznego* wydanej w 2013 r. znajdował się na innym etapie rozwoju.

W 2020 r. opublikowano *Białą Księgę* dotyczącą sztucznej inteligencji (AI) i cyfryzacji. Ma ona stanowić klucz do zwalczenia cyberterroryzmu i osiągnięcia ładu klimatycznego przez doskonalenie AI[655]. To konieczny element pozwalający na utrzymanie jednolitego rynku UE dzięki badaniom naukowym, innowacjom i wdrożeniu do grudnia 2020 r. skoordynowanego planu działań w ramach programów *Cyfrowa Europa* oraz *Horyzont Europa* na lata 2021–2027.

Konieczne jest opracowanie planu szybkiego reagowania państw członkowskich, który umożliwi natychmiastową, skuteczną i skoordynowaną reakcję w przypadkach wystąpienia ataków cybernetycznych na dużą skalę, a także pogłębienie współpracy międzynarodowej. Wprowadzając ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne wspierające strategiczne ramy zapobiegania konfliktom i stabilizacji w cyberprzestrzeni, UE wzmocni swoją zdolność reagowania na cyberataki,

Problem normalizacji dostawców usług cyfrowych powinien zostać rozwiązany w ten sposób, że zainteresowany właściwy organ powinien podejmować działania wyłącznie wtedy, gdy otrzymał dowód, np. od dostawcy usług cyfrowych, innego właściwego organu,

w tym właściwego organu innego państwa członkowskiego, lub od użytkownika usługi, że dostawca usług cyfrowych nie spełnia wymogów niniejszej dyrektywy, w szczególności w wyniku wystąpienia incydentu. Właściwy organ nie powinien mieć ogólnego obowiązku nadzorowania dostawców usług cyfrowych.

We wszystkich państwach UE dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii z dnia 6 lipca 2016 r.[656], zwana dalej dyrektywą NIS, jest wprowadzona szerzej, niż wynika to z jej zapisu. W przypadku Polski uwzględniono dodatkowe sektory takie, jak energetyczny i węglowy, a także związane ze zdrowiem i bakowością. Zgodnie z art. 1 ustawy i art. 1 dyrektywy 2016/1148 nie ma ona zastosowania wobec przedsiębiorców telekomunikacyjnych i dostawców usług zaufania, którzy zostali już objęci europejskimi i krajowymi wymaganiami sektorowymi z zakresu cyberbezpieczeństwa[657].

W przepisach ogólnych, szczególnie art. 2. ustawy określono zakres regulacji, słowniczek pojęć ustawowych, katalog podmiotów tworzących krajowy system cyberbezpieczeństwa oraz cele projektowanej ustawy. Ustawa określa organizację polskiego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy, zakres oraz tryb stanowienia *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej*[658].

Należy również zauważyć, że zgodnie z art. 288 TL[659] transpozycja przepisów wprost co do dyrektywy do prawa krajowego nie jest rozwiązaniem przyjętym przez ustawodawcę unijnego. Priorytetem jest spójność krajowego systemu prawa z prawem unijnym.

Definicja bezpieczeństwa informacji w dyrektywie NIS rozszerzyła trzy podstawowe atrybuty: poufność, integralność i dostępność o czwarty atrybut – autentyczność, która polega na tym, że podmiot jest tym, za kogo się podaje[660].

Ustawa wprowadza pojęcie sektorowego zespołu cyberbezpieczeństwa[661], czyli zespołu ustanowionego przez organ

właściwy dla danego sektora lub podsektora wymienionego w załączniku do ustawy, odpowiedzialnego za obsługę lub wsparcie obsługi incydentów w danym sektorze lub podsektorze.

Polski ustawodawca zdefiniował cyberbezpieczeństwo w art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa jako odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[662].

Dyrektywa NIS przyjęła nową definicję systemów i sieci teleinformatycznych obejmującą:

- sieci łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE;
- wszelkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych lub dane cyfrowe przechowywane, przetwarzane, odzyskiwane lub przekazywane w celu ich eksploatacji, użycia, ochrony i utrzymania[663].

Należy też wskazać na definicje związane z szacowaniem ryzyka i zagrożeniami. Ustawa definiuje ryzyko[664], szacowanie ryzyka[665], zarządzanie ryzykiem[666], zagrożenie cyberbezpieczeństwa[667] i podatność[668].

W rozumieniu ustawy i dyrektywy NIS istnieją trzy usługi cyfrowe:

- internetowa platforma handlowa,
- przetwarzanie w chmurze,
- wyszukiwarka internetowa[669].

Definicja usługi przetwarzania w chmurze została skonstruowana na podstawie terminów technologicznych, a nie prawnych, dlatego należy odczytywać ją razem z motywami dyrektywy NIS i definicją usługi cyfrowej. Usługa przetwarzania w chmurze dotyczy tylko usług świadczonych przez dany podmiot swoim klientom. Wyłączone są zatem przypadki chmury prywatnej, która jest usługą świadczoną

wewnątrz organizacji. Z kolei w art. 3 zostały określone cele polskiego systemu cyberbezpieczeństwa, którymi będą niezakłócone świadczenie usług kluczowych i usług cyfrowych, osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.

Artykuł 4 wskazuje podmioty, które obejmuje krajowy system cyberbezpieczeństwa, a więc podmioty zobowiązane, podmioty realizujące techniczne, organizacyjne i administracyjno-regulacyjne zadania w systemie, jednostki sektora finansów publicznych. System będzie zatem obejmować m.in. operatorów usług kluczowych, dostawców usług cyfrowych, zespoły CSIRT, sektorowe zespoły cyberbezpieczeństwa, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe ds. cyberbezpieczeństwa, pojedynczy punkt kontaktowy ds. cyberbezpieczeństwa, pełnomocnika rządu ds. cyberbezpieczeństwa i kolegium ds. cyberbezpieczeństwa, instytuty badawcze, a także jednostki sektora finansów publicznych objęte zakresem ustawy. W przepisach szczegółowych zostały natomiast opisane uprawnienia i obowiązki tych podmiotów, jak również zakres przypisanej im odpowiedzialności[670].

Uwzględniono również konieczność objęcia ustawą niektórych podmiotów wymienionych w art. 9 pkt 14 ustawy o finansach publicznych (tzw. inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych). Należą do nich: Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej. Ustawą zostaną również objęte spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej[671].

* * *

Częstotliwość oraz rozwój nowych technologii i zagrożeń znacznie przewyższa implementację prawodawstwa UE. Procedury Unii nie zostały zaprojektowane z myślą o erze cyfrowej. Opracowywanie innowacyjnych i elastycznych procedur w celu zapewnienia polityki i ram prawnych, które są odpowiednie do wyznaczonego celu strategicznego, aby lepiej przewidywać i kształtować przyszłość, jest zadaniem kluczowym. Mimo dążenia do większej spójności ramy prawne dotyczące cyberbezpieczeństwa pozostają niekompletne.

Fragmentacja i luki utrudniają osiągnięcie ogólnych celów polityki i prowadzą do nieefektywności. Może to przyczyniać się do zjawiska „nadregulacji", ponieważ art. 73 TFUE wyraźnie dopuszcza możliwość stanowienia norm prawnych za zgodą państw na szczeblu unijnym. Jednocześnie, zgodnie z art. 75 TFUE, to zwalczanie terroryzmu i cyberterroryzmu znalazło się w obszarze kompetencji dzielonych UE i państw członkowskich, obszar cyberobrony jest natomiast podstawowym zadaniem i kompetencją państwa w polityce wewnętrznej państwa członkowskiego, co wynika z art. 4 wzw. 72 TFUE. Unii przyznano prawo do stanowienia strategii bezpieczeństwa w myśl art. 68 TFUE. W tej sytuacji prawnej państwa mogą, ale nie muszą uregulować kwestie związane z polityką cyberobrony. Na szczeblu unijnym może dojść do zjawiska nadregulacji i kolizji przepisów prawnych, co negatywnie wpłynie na proces usprawniania współpracy między państwami.

Braki zidentyfikowane przez Komisję w ocenie strategii obejmowały Internet[672], równowagę obowiązków między użytkownikami a dostawcami produktów cyfrowych oraz to, że niektóre aspekty nie zostały uwzględnione w dyrektywie w sprawie bezpieczeństwa sieci i informacji (NIS). Polityka cyberbezpieczeństwa stara się rozwiązać ten problem po części przez promowanie bezpieczeństwa w fazie projektowania za pomocą szerokiego systemu certyfikacji. Niektórzy interesariusze uważają, że jasno zdefiniowany cyberprzemysł polityki i wspólnego podejścia do cyberszpiegostwa są nadal nieobecne[673].

Stosowanie niektórych aspektów ustawodawstwa pozostaje dobrowolne na poziomie władz i podmiotów prywatnych, np. w

ramach Grupy Współpracy oceniającej krajowe strategie bezpieczeństwa sieci, systemy informacyjne i skuteczność CSIRT. Proponowany system certyfikacji w dyrektywie NIS czy stosowanie certyfikacji dla produktów i usług ICT również jest dobrowolne. Poza tym dyrektywy UE dotyczące podmiotów prywatnych nie nakładają żadnych szczegółowych wymogów ujawniania zagrożenia cybernetycznego. Różne podejście państw członkowskich do zaangażowania we współpracę i podawanie wrażliwych informacji (dotyczących bezpieczeństwa narodowego) także nie jest dobrym rozwiązaniem.

Cyberbezpieczeństwo w UE jest prerogatywą państw członkowskich w przeciwieństwie do cyberterroryzmu, który należy do kompetencji dzielonych. Mimo to UE ma do odegrania kluczową rolę w tworzeniu warunków dla zdolności państw członkowskich, aby ulepszać, współpracować i budować zaufanie.

Niespójna transpozycja prawa UE między państwami członkowskimi może skutkować niespójnościami operacyjnymi i uniemożliwieniem osiągnięcia pełnego potencjału prawodawstwa. Ponadto ochrona prywatności i wolności słowa wymaga dostosowania odpowiedniego ustawodawstwa w celu znalezienia niezbędnej równowagi między ochroną wartości podstawowych i realizacji celów bezpieczeństwa UE. Możemy np. osiągnąć cele RODO i jednocześnie mieć wpływ na publiczny dostęp do informacji na temat rejestrujących nazwy domen oraz posiadaczy bloków adresów IP? Czy może to niekorzystnie wpłynąć na egzekwowanie prawa procesowego w śledztwie? Samo prawodawstwo nie gwarantuje odporności. Celem dyrektywy NIS jest osiągnięcie wysokiego poziomu bezpieczeństwa w całej UE.

Na podstawie przeprowadzonej analizy należy stwierdzić, że skuteczność działań podejmowanych przez organy UE w zakresie polityki cyberterrorystycznej zależy od rodzaju instrumentów będących w dyspozycji UE i państw członkowskich oraz podstawy prawnej odpowiednich regulacji. Na efektywność danego instrumentu wpływa jego prosty mechanizm funkcjonowania, sposób jego uchwalenia, zakres jego obowiązywania wobec państw

członkowskich, bezpośredniość skutku bądź jego brak oraz mechanizmy kontroli nad jego przestrzeganiem[674].

Kolejnym problemem jest brak powszechnie stosowanych, znormalizowanych sposobów poziomej oceny bezpieczeństwa oprogramowania, oprócz niektórych metod przeprowadzania testów penetracyjnych lub przeglądu kodu. Sytuacja wygląda gorzej, jeśli weźmiemy pod lupę sposób certyfikacji bezpieczeństwa oprogramowania.

Patrząc z ogólnej perspektywy na realizację polityki cyberbezpieczeństwa i działania podejmowane przez UE, ocena jest raczej negatywna. Najbardziej prawdopodobnym powodem takiego rozpoznania jest to, że europejskie ambicje i oczekiwania w walce z cyberterroryzmem są zbyt wysokie w porównaniu z rzeczywistością. Chociaż przygotowano stosowne przepisy mające służyć przeciwdziałaniu cyberterroryzmowi (NIS czy RODO), problemem jest niechęć do współpracy między państwami członkowskimi a UE, zwłaszcza gdy jest od nich wymagana rezygnacja z kompetencji na szczeblu państwowym w zakresie cyberbezpieczeństwa, oraz nieprecyzyjny podział kompetencji między Unię a państwa członkowskie.

Polityka cyberbezpieczeństwa Unii Europejskiej powinna zatem zmierzać do wskazania nowych przyczyn tego zjawiska oraz stworzenia zintegrowanego systemu obronnego cyberprzestrzeni zarówno na terenie poszczególnych państw, jak i całej UE. Wprawdzie dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[675] w dniu 6 lipca 2016 r. (zwana dalej dyrektywą 2016/1148 lub dyrektywą NIS) zobowiązała wszystkie państwa członkowskie UE do zagwarantowania minimalnego poziomu zdolności krajowych w dziedzinie cyberbezpieczeństwa przez ustanowienie organów właściwych oraz pojedynczego punktu kontaktowego ds. cyberbezpieczeństwa, powołanie zespołów reagowania na incydenty komputerowe (CSIRT) oraz przyjęcie państwowych strategii w zakresie cyberbezpieczeństwa, jednak w

obecnych uwarunkowaniach należałoby się posługiwać zarówno wysoce wyspecjalizowanymi narzędziami informatycznymi, jak i lepszymi instytucjami na szczeblu unijnym. Ponadto zbyt wąskie kompetencje w tej dziedzinie ENISY czy Eurojustu nie dają szansy na szybką współpracę w obszarze zwalczania cyberterroryzmu. Wprowadzenie odpowiednich przepisów prawnych z pewnością zmniejszyłoby ryzyko wystąpienia tego zjawiska, jednak go nie zniweluje. Trudność leży głównie po stronie prawnej.

Należy pamiętać, że nawet najlepsze zabezpieczenia techniczne i regulacje prawne na nic się zdadzą, jeżeli nie będą iść w parze z działaniem odpowiednich instytucji i rozwagą użytkowników. I w tym przypadku potwierdza się reguła, że człowiek stanowi najważniejsze, a zarazem najsłabsze ogniwo w systemie zabezpieczeń. Brak spójnych ram zarządzania cyberbezpieczeństwem osłabia zdolność społeczności międzynarodowej do reagowania na cyberataki i ich ograniczania. Dlatego należy wypracować konsensus w sprawie takich ram zarządzania, które są najlepszym odzwierciedleniem interesów i wartości UE.

Bardzo ważna jest również potrzeba prowadzenia działań edukacyjnych. Powinny one polegać na upowszechnianiu wiedzy na temat zagrożeń i świadomości użytkowników dotyczących możliwości minimalizowania ryzyka związanego z korzystaniem z cyberprzestrzeni[676].

6

IMPLEMENTACJA POLITYKI CYBERBEZPIECZEŃSTWA W UNII EUROPEJSKIEJ NA PRZYKŁADZIE WYBRANYCH PAŃSTW

Szósty rozdział został poświęcony implementacji polityki i strategii cyberbezpieczeństwa w wybranych państwa członkowskich UE. Podmiotami analizy będą: Estonia, Francja, Niemcy, Polska i Wielka Brytania. Wybór powyższych państw umożliwi wykazanie różnic i podobieństw w strategiach i politykach państw członkowskich w zakresie zwalczania tego zjawiska. Tym samym analiza implementacji polityki cyberbezpieczeństwa na przykładzie wybranych państw umożliwi poznanie strategii krajowych i instrumentów, za pomocą których państwa realizują funkcje ochronne na poziomach wewnątrzpaństwowym i europejskim, a tym samym implementują politykę cyberbezpieczeństwa na swój poziom. Przedstawione i ocenione instrumenty stosowane przez wybrane państwa w prowadzonych przez nich politykach cyberbezpieczeństwa zostaną poddane ocenie. To z kolei pozwoli na poznanie zależności problemów bezpieczeństwa wewnętrznego UE, a tym samym polityki cyberbezpieczeństwa, od poziomu integracji państw członkowskich.

Należy zaznaczyć, że termin „implementacja” nie jest jednakowo rozumiany w poszczególnych państwach członkowskich Unii Europejskiej. W dużym uproszczeniu można stwierdzić, że

implementację prawa unijnego można wiązać z czynnościami, które umożliwiają rzeczywiste wprowadzenie w życie postanowień przyjętych na szczeblu unijnym do państwowych porządków prawnych. Proces scalania prawa unijnego z prawem państw członkowskich jest dość skomplikowany i w pojęciu węższym również nosi nazwę implementacji prawa unijnego. Aby państwa członkowskie mogły korzystać z dobrodziejstw członkostwa w Unii Europejskiej, muszą dokonać sprawnej i skutecznej transpozycji prawa UE na grunt krajowy, która polega na podejmowaniu wszelkich działań, aby zapewnić efektywne stosowanie i przestrzeganie prawa unijnego w krajowych porządkach prawnych.

Z tego względu pojęcie implementacji prawa nie obejmuje jedynie działań stricte legislacyjnych podejmowanych w poszczególnych państwach członkowskich, lecz także wszelkie czynności krajowych organów, mające na celu skuteczne stosowanie norm unijnych zawartych w dyrektywie. Implementacja dyrektywy zawiera całokształt działań podejmowanych na szczeblu państwowych, mających na celu przeniesienie założeń regulacji unijnej do wewnętrznego systemu prawnego przy uwzględnieniu jego specyfiki.

6.1
IMPLEMENTACJA POLITYKI CYBERBEZPIECZEŃSTWA W ESTONII

6.1.1. PODSTAWOWE DOKUMENTY W ZAKRESIE POLITYKI CYBERBEZPIECZEŃSTWA

Estonia ratyfikowała *Konwencję Rady Europy o cyberprzestępczości*[677] w 2003 r., wprowadzając do kodeksu karnego przepisy dotyczące takich przestępstw, jak (§ 137 k.k.) nielegalne przechwytywanie danych, sabotaż komputerowy polegający w rozumieniu prawa estońskiego na nielegalnej zmianie, usuwanie, uszkadzanie lub blokowanie danych w systemach komputerowych (§ 206 k.k.), celowe uszkodzenie

połączeń do sieci komputerowej bądź systemu komputerowego (§ 207), rozpowszechnianie wirusów komputerowych (§ 208 k.k.), niedozwolone uzyskanie dostępu do komputera bądź sieci komputerowej (§ 217 k.k.) czy oszustwa komputerowe (§ 213 k.k.). Nowelizacja estońskiego kodeksu karnego wprowadziła przepis penalizujący cyberataki z rozróżnieniem na ataki na infrastrukturę krytyczną (w celu poważnego wpłynięcia bądź zniszczenia ekonomicznej albo społecznej struktury państwa) oraz na zwykłe przestępstwa komputerowe. Zmiany zaszły również w procedurze karnej, gdzie zmieniono postanowienia dotyczące pozyskiwania dowodów, w tym dowodów cyfrowych[678]. *Estoński kodeks postępowania karnego*[679] nie stanowi odrębnych przepisów dotyczących ścigania osób za akty cyberterroryzmu. Osoby podejrzane o jakikolwiek akt terrorystyczny mają te same prawa i podlegają tym samym zasadom proceduralnym, jak osoby podejrzane o popełnienie innego przestępstwa.

Kolejną konsekwencją przystąpienia do konwencji budapeszteńskiej i wprowadzenia zmian w kodeksie karnym było przyjęcie ustawy o łączności elektronicznej 8 grudnia 2004 r.[680] Miała ona na celu stworzenie warunków niezbędnych do rozwoju komunikacji elektronicznej, aby promować rozwój komunikacji elektronicznej sieci i usług komunikacyjnych bez preferowania określonych technologii, oraz zapewnienie ochrony interesów użytkowników usług łączności elektronicznej przez promowanie wolnej konkurencji, a także celowego i sprawiedliwego planowania, przydzielania i użytkowania radia, częstotliwości i numeracji[681].

Kolejnym aktem prawnym przyjętym przez Estonię była ustawa o ochronie danych osobowych z dnia 6 grudnia 2007 r.[682] regulująca procedurę przechowywania i dostępu do danych osobowych, a także tryb wykonywania nadzoru państwowego nad przetwarzaniem danych osobowych.

Estonia jest jednym z najbardziej zaawansowanych technologicznie państw członkowskich Unii Europejskiej[683]. Tak jak wiele innych wysoko rozwiniętych państw, Estonia w dużej mierze jest zależna od niezakłóconego działania systemów komputerowych i źródeł komunikacji. Wydarzenia sprzed kilku lat[684] przyczyniły się

bezpośrednio do zmiany prawa oraz powołania nowych instytucji mających na celu efektywną walkę z zagrożeniami w cyberprzestrzeni[685]. Ustanowiona w Estonii w 2009 r. ustawa o zarządzaniu awaryjnym stanowiła przegląd bieżącej konfiguracji narodowej gotowości i struktury zarządzania awaryjnego w zakresie związanym z zagrożeniami cybernetycznymi. Ustawa stanowiła kompleksowe podejście do problemu zarządzania kryzysowego: regulowała zapobieganie, przygotowanie, reagowanie na sytuacje awaryjne oraz łagodzenie skutków katastrofy. Nakładała na dostawców usług publicznych i właścicieli infrastruktury obowiązki zapewniające zapobieganie sytuacjom kryzysowym oraz zapewnienie stabilnego poziomu ciągłości usług. Dostawcy usług zostali zobowiązani m.in. do przygotowywania i przedstawiania oceny ryzyka, informowania obywateli o zdarzeniach istotnie wpływających na ciągłość świadczonych usług.

Estoński rząd we wrześniu 2014 r. zatwierdził *Strategię cyberbezpieczeństwa na lata 2014–2017*, która była kontynuacją *Strategii cyberbezpieczeństwa na lata 2008–2013*[686]. Strategia z 2008 r. była pierwszym krajowym dokumentem uznającym interdyscyplinarny charakter cyberbezpieczeństwa i potrzebę skoordynowania działań w tym obszarze. Była to również jedna z pierwszych horyzontalnych strategii cyberbezpieczeństwa na świecie i dowodziła, że od tego momentu cyberbezpieczeństwo zaczęło być postrzegane jako istotny element bezpieczeństwa narodowego.

W *Strategii cyberbezpieczeństwa Estonii na lata 2014–2017*[687] główne zagrożenia bezpieczeństwa cybernetycznego zidentyfikowano jako rosnące uzależnienie od infrastruktury ICT i e-usług przez państwo, gospodarkę i społeczeństwo. Kluczowymi obszarami stało się zapewnienie dostępu do podstawowych usług, skuteczniejsze zwalczanie cyberprzestępczości i pogłębianie narodowych zdolności obronnych. Dodatkowe działania wspierające obejmowały: kształtowanie ram prawnych, promowanie międzynarodowej współpracy i komunikacji, podnoszenie świadomości oraz zapewnienie kształcenia specjalistycznego, a także rozwój rozwiązań technicznych[688].

Uznano, że strategia cyberbezpieczeństwa Estonii:

- stanowi integralną część bezpieczeństwa narodowego, wspomaga prawidłowe funkcjonowania państwa i społeczeństwa, konkurencyjność gospodarki oraz innowacje;
- gwarantuje poszanowanie podstawowych praw i wolności, a także chroni wolność jednostki, dane osobowe i tożsamość;
- działa, opierając się na zasadzie proporcjonalności, przy uwzględnieniu istniejących i potencjalnych zagrożeń i zasobów;
- działa w sposób skoordynowany przez współpracę sektora publiczno-prywatnego oraz trzeciego sektora, z uwzględnieniem wzajemnych powiązań i współzależności między istniejącą infrastrukturę a usługami w przestrzeni wirtualnej;
- rozpoczyna się od indywidualnej odpowiedzialności za bezpieczne korzystanie z narzędzi ICT;
- za priorytet uznaje zapewnienie bezpieczeństwa cybernetycznego oraz zapobieganie potencjalnym zagrożeniom i skuteczne reagowanie na zagrożenia, które należy zmaterializować;
- musi być wspomagana przez międzynarodowe trendy badań i rozwoju;
- zapewnia cyberbezpieczeństwo państwa przez międzynarodową współpracę z sojusznikami i partnerami[689].

W 2015 r. estoński parlament uchwalił ważną ustawę *National Defence Act*[690], która kompleksowo uregulowała obowiązki poszczególnych organów państwa. Główne zadanie powierzono Radzie Obrony Narodowej działającej przy prezydencie oraz Komisji Bezpieczeństwa Rządu Państwa, a także innym instytucjom rządowym i samorządowych w zakresie obrony narodowej. Ten akt prawny wprowadził nowy system dowodzenia godnie z zasadą, że wszystkie instytucje władzy publicznej będą wykonywać te same funkcje w czasie pokoju, kryzysu i wojny. W ten sposób również zarządzanie cyberbezpieczeństwem zostało ujęte w sposób jednolity, niemniej jednak to organy centralne sprawowały nadzór nad pozostałymi instytucjami.

9 maja 2018 r. parlament uchwalił nową ustawę *Cybersecurity Act*[691], która nie tylko implementuje dyrektywę PE w sprawie bezpieczeństwa sieci i systemów informatycznych (NIS), ale przede wszystkim

ustanawia zasady i procedury dotyczące systemu cyberbezpieczeństwa Republiki Estonii. Reguluje odpowiedzialność organów administracji państwowej, w tym Ministerstwa Spraw Gospodarczych i Łączności, oraz nadzór nad systemami informatycznymi. Ponadto określa rolę urzędu Information System Authority (RIA) i ma na celu przygotowanie środków do zapewnienia ciągłości funkcjonowania cyfrowych usług również w sytuacji utraty kontroli nad częścią lub całością terytorium państwa[692].

Rok później przyjęto *Strategię cyberbezpieczeństwa Estonii na lata 2019–2022*[693] będącą kontynuacją poprzedniej. W dokumencie tym zapisano, że cyberbezpieczeństwo jest powszechnie akceptowane jako integralna część funkcjonowania państwa, gospodarki, bezpieczeństwa wewnętrznego i zewnętrznego. Podkreślono również, że społeczeństwo estońskie nie jest odpowiednio przygotowane do radzenia sobie z istniejącymi cyberzagrożeniami w sektorach prywatnym i publicznym, będąc w dużej mierze nieświadome zagrożeń i potrzeb. Uznano, że do końca 2022 r. Estonia osiągnie następujące cele:

- zrównoważone społeczeństwo cyfrowe,
- bezpieczeństwo cybernetyczne przez przemysł, badania i rozwój,
- stanie się wiodącym międzynarodowym współpracownikiem,
- będzie cyberpoznawcą społeczeństwa informacyjnego.

Zgodnie z założeniem *National Security Concept* cyberbezpieczeństwo[694] jest integralną częścią obrony militarnej Estonii realizującej strategiczne cele w Estońskich Siłach Obrony. Dlatego w sierpniu 2018 r. powołano Dowództwo Cyberobrony podporządkowane bezpośrednio Dowódcy Estońskich Sił Obrony. Do głównych zadań Dowództwa Cyberobrony należy m.in. przeprowadzanie operacji w cyberprzestrzeni, zapewnienie odpowiedniej infrastruktury oraz usług IT na potrzeby Estońskich Sił Obrony, analiza sytuacji w cyberprzestrzeni, badania i rozwój w zakresie cyberbezpieczeństwa oraz szkolenie jednostek Estońskich Sił Obrony. Dowództwo Cyberobrony ma osiągnąć pełną zdolność operacyjną do 2023 r.

Powołano również Estońską Cyber Unit Estońskiej Ligi Obrony składającą się z wolontariuszy, a jej misją jest wsparcie ochrony estońskiej cyberprzestrzeni i infrastruktury informacyjnej. Jednostka skupia specjalistów w zakresie bezpieczeństwa cybernetycznego oraz ekspertów z innych dziedzin, w tym prawników, ekonomistów, politologów itp. Ważnym aspektem funkcjonowania Cyber Unit jest też włączenie młodzieży z umiejętnościami w dziedzinie IT do działań w zakresie obrony estońskiej cyberprzestrzeni (z podkreśleniem patriotycznego aspektu tej aktywności). Cyber Unit jest dobrym przykładem, jak w umiejętny sposób zaangażować społeczeństwo (zwłaszcza ludzi młodych) do pomocy w obronie państwa (w tym przypadku cyberprzestrzeni)[695].

Strategia z 2019 r. koncentruje się na przejściu do proaktywnych usług, które zapewniają wsparcie ze strony państwa, gdy jest to niezbędne. Przewiduje sprawniejsze administrowanie usługami publicznymi, rozwój elementów infrastruktury w państwie cyfrowym oraz systematyczne testowanie nowych rozwiązań, z udziałem środowiska akademickiego i sektora prywatnego, w tym start-upów.

Wykorzystanie sztucznej inteligencji w estońskim sektorze publicznym już się rozpoczęło. Aby komunikacja obywatela i przedsiębiorcy z państwem była łatwiejsza i wygodniejsza, wdrażana jest koncepcja tzw. biurokraty, która zakłada stworzenie wirtualnego asystenta. Ten asystent, który rozumie i mówi po estońsku, ułatwia korzystanie z usług państwowych, ponieważ jest zintegrowany z najważniejszymi e-usługami wszystkich obszarów administracyjnych. Jednocześnie każdy obywatel musi być w stanie korzystać ze wszystkich usług publicznych bez specjalnej wiedzy, przy użyciu odpowiedniej metody i urządzenia do komunikacji, a coraz częściej także poza granicami Unii Europejskiej.

6.1.2. INSTYTUCJONALNY WYMIAR POLITYKI CYBERBEZPIECZEŃSTWA

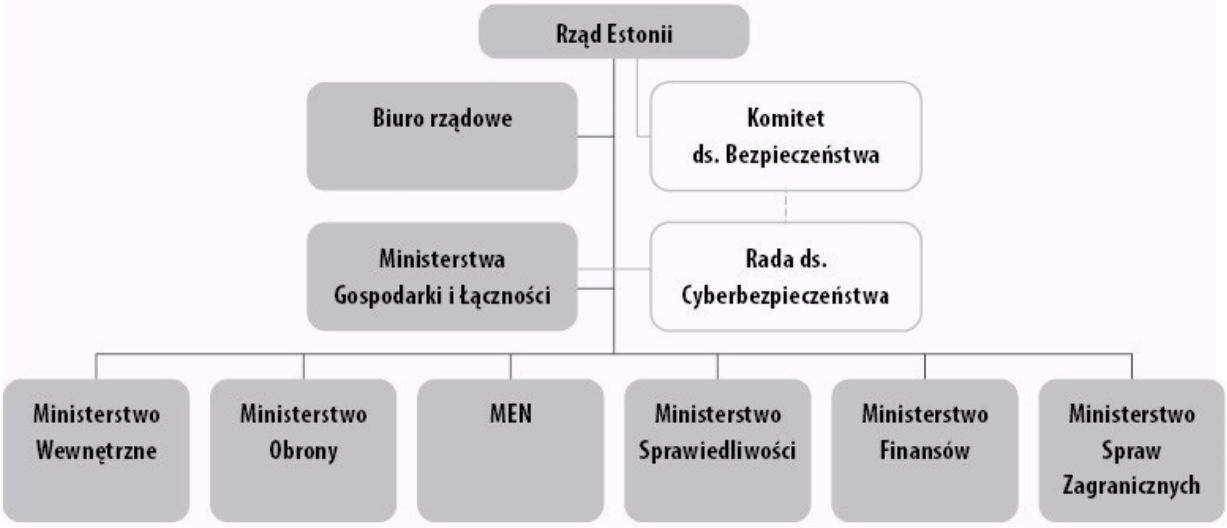
Na skutek doznanych ataków już w 2009 r. w Komitecie Bezpieczeństwa Estonii powołano Radę Cyberbezpieczeństwa, która miała odpowiadać za wspieranie różnych agencji na poziomie

strategicznym oraz nadzorować realizację strategii bezpieczeństwa. Estońskiemu Centrum Informatycznemu w 2010 r. nadano status agencji rządowej i zmieniono nazwę na Estoński Urząd Systemu Informacji (est. *Riigi Infosüsteemi Amet*, RIA). RIA otrzymał uprawnienia do organizowania ochrony sieci informacyjno-komunikacyjnych, w tym infrastruktury krytycznej państwa, a także do wymiany informacji operacyjnych, identyfikacji problemów i rekomendowania kierunków poprawy bezpieczeństwa infrastruktury krytycznej państwa. Estońska Agencja Bezpieczeństwa Wewnętrznego postawiła sobie za cel wzmocnienie swoich zdolności dochodzeniowych w celu zapobiegania zagrożeniom bezpieczeństwa narodowego, w tym cyberataków i szpiegostwa.

Dobrym rozwiązaniem było również powołanie Jednostki Estońskiej Ligi Cyberobrony, tzw. cyberarmii czy cyberrezerwy, pozostającej w gotowości w przypadku wystąpienia cyberataku. Przyjęcie tego rozwiązania daje możliwość szybkiej reakcji na zagrożenie, dlatego tożsame regulacje mogą w niedługim czasie pojawić się w innych państwach. Ta dobrowolna organizacja zrzesza obywateli, mając na celu ochronę estońskiej cyberprzestrzeni. Jednostka składa się ze specjalistów w kluczowych zagadnieniach cyberbezpieczeństwa, głównie informatyków, lecz również prawników.

Misją EDL CU jest ochrona infrastruktury krytycznej, wspieranie szerszych celów obrony narodowej, podniesienie poziomu bezpieczeństwa cybernetycznego przez edukację społeczeństwa i szkolenia, utworzenie sieci, która ułatwia partnerstwo publiczno-prywatne i zwiększa gotowość do działania podczas sytuacji kryzysowych. Wiedza ochotników EDL CU jest stosowana w celu poprawy bezpieczeństwa systemów informacyjnych estońskich instytucji państwowych i firm przez skoordynowanie ćwiczeń oraz testowanie rozwiązań i szkoleń.

Obecny system zarządzania cyberbezpieczeństwem w Estonii przedstawiono na *rys. 6.1*.



RYSUNEK 6.1 System zarządzania strategią cyberbezpieczeństwa w Estonii

Źródło: Cyber Security Strategy 2019–2022, Ministry of Economic Affairs and Communication 2019, s. 36.

Planowanie polityki cyberbezpieczeństwa i realizacja strategii są skoordynowane. Koordynacja odbywa się za pośrednictwem rządu, Republiki Rady ds. Cyberbezpieczeństwa, Komitetu ds. Bezpieczeństwa oraz Ministerstwa Gospodarki i Łączności, które zapewnia wdrożenie celów strategii cyberbezpieczeństwa za pośrednictwem odpowiedniej instytucji rządowej przez dokumenty planistyczne, instytucje, programy i plany pracy. Główna odpowiedzialność za realizację ogólnokrajowej polityki cybernetycznej w strategii cyberbezpieczeństwa należy do instytucji rządowych, które wnoszą swój wkład do prac Rady ds. Cyberbezpieczeństwa.

Ministerstwo Edukacji i Badań bierze pod uwagę uzgodnione priorytety w celach strategii bezpieczeństwa cybernetycznego w planowaniu strategii uczenia się przez całe życie. Prowadzi działania wspierające zdobywanie przez absolwentów podstawowej wiedzy o charakterze edukacyjnym na różnych poziomach, aby mogli radzić sobie z zagrożeniami cybernetycznymi. Ministerstwo jest wspierane przez Information Technology Foundation for Education (HITSA), która przyczynia się do szkolenia specjalistów w tej dziedzinie przez koordynację programu Targalt Internetis (*Staying Smart Online*) oraz programu Akademia IT.

Ministerstwo Sprawiedliwości współpracuje z Prokuraturą Generalną, która kieruje przedprocesowym postępowaniem karnym. Wnosi swój wkład do planowania polityki sądowej i karnej w całym sektorze i przez działania w zakresie strategii zapobiegania przemocy. Planuje działania profilaktyczne i sektorowe. Instytucje uznane za ważne z punktu widzenia cyberbezpieczeństwa w obszarze administracyjnym Ministerstwa Sprawiedliwości to Inspektorat Ochrony Danych (AKI), który sprawuje nadzór nad uprawnieniami i obowiązkami w zakresie ochrony danych osobowych, estoński Instytut Kryminalistyki (EKEI), który zajmuje się ekspercką analizą technologii informatycznych.

Ministerstwo Obrony Narodowej we współpracy z Siłami Obrony, Ligą Obrony oraz Służbami Wywiadu Zagranicznego odpowiada za realizację działań dotyczących obrony wojskowej i przyczynia się przez cały czas do tworzenia międzysektorowych mechanizmów współpracy i koordynacji. Centrum Informatyki i Rozwoju Ministerstwa Spraw Wewnętrznych (SMIT) zapewnia administrację i rozwój systemów informatycznych związanych z bezpieczeństwem krajowym.

Ministerstwo Spraw Zagranicznych kieruje współpracą międzynarodową związaną ze strategią i koordynuje ją. Ministerstwo Finansów bierze udział w opracowywaniu różnych części strategii, w tym zapewnia trwałość i integrację z innymi procesami planowania strategicznego. Komisja Nadzoru Finansowego angażuje się w cyberbezpieczeństwo, sprawując nadzór nad instytucjami finansowymi.

Biuro rządowe zapewnia, że cyberbezpieczeństwo jest zintegrowane z obroną narodową i ujęte w dokumentach planistycznych (plan rozwoju obronności kraju i obronność państwa).

6.2
IMPLEMENTACJA POLITYKI CYBERBEZPIECZEŃSTWA W POLSCE

6.2.1. PODSTAWOWE DOKUMENTY W ZAKRESIE POLITYKI CYBERBEZPIECZEŃSTWA

Strategia Bezpieczeństwa Narodowego (SBN) z 2014 r.[696] była jednym z najważniejszych dokumentów tej rangi w Polsce. Przyczynia się do zapewnienia bezpieczeństwa państwa i obywateli, a tym samym gwarantuje stabilny rozwój kraju i pomnożenie bogactwa jego mieszkańców. Jest także wskazaniem kierunków rozwoju organów, które będą odpowiedzialne za bezpieczeństwo państwa, również jego militarną stronę. Dokument stanowi podstawę do działań dla Ministerstwa Obrony Narodowej (MON) w kierunku transformacji Sił Zbrojnych Rzeczypospolitej Polskiej (SZ RP) przeciwko nowym wyzwaniom współczesnego pola walki we wszystkich jego obszarach: na wodzie i na lądzie, w powietrzu i w kosmosie oraz w cyberprzestrzeni[697].

Analiza treści strategii pozwala określić różne obszary bezpieczeństwa: regionalne, globalne oraz krajowe, ważne dla funkcjonowania państwa w nowych uwarunkowaniach geopolitycznych i społecznych. W dokumencie zdiagnozowano także zagrożenia nowego typu, m.in. cyberzagrożenia. Wraz z pojawieniem się nowych technologii teleinformatycznych oraz rozwojem sieci Internet pojawiły się takie zagrożenia jak cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty z udziałem podmiotów niepaństwowych i cyberwojna, rozumiana jako konfrontacja w cyberprzestrzeni między państwami[698]. Kierunki rozwoju zagrożeń w cyberprzestrzeni wyraźnie wskazują na rosnący wpływ poziomu bezpieczeństwa obszaru domeny cyfrowej na bezpieczeństwo ogólne państwa. Przy rosnącym uzależnieniu od technologii teleinformatycznych konflikty w cyberprzestrzeni mogą poważnie zakłócić funkcjonowanie społeczeństw i państw.

12 maja 2020 r. w drodze postanowienia[699] Prezydent RP zatwierdził nową *Strategię Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*. Tym samym z dniem zatwierdzenia nowej Strategii *Strategia Bezpieczeństwa Narodowego RP* z 5 listopada 2014 r. straciła moc[700].

Strategia z 2020 r. ma nieco inny układ i strukturę niż jej poprzedniczki z 2007 i 2014 r. Rozpoczyna się od oceny środowiska, a nie od identyfikacji interesów narodowych. Zajmuje się wprawdzie interesami narodowymi, ale nie są one jej punktem wyjścia. W sposób właściwy i wyczerpujący odnotowuje najistotniejsze kwestie współczesnego środowiska bezpieczeństwa. Słusznie akcentuje zagrożenia ze strony Rosji. Jest to ważne nie tylko dla ukierunkowania narodowych przygotowań, ale także dla akcentowania w relacjach z sojusznikami wagi problemu bezpieczeństwa wschodniej flanki NATO i UE. Sygnalizuje ryzyka związane z wewnętrznymi kłopotami NATO i UE. Z tego powinna wynikać potrzeba ewentualnościowych analiz różnych przyszłościowych scenariuszy polityczno-strategicznych dla Polski. Ponadto zauważono ryzyko konfliktu hegemonicznego na linii USA – Chiny.

Dostrzega wszystkie najnowsze trendy i nurty w rozwoju warunków bezpieczeństwa, odnotowując takie kwestie, jak hybrydowość zagrożeń, w tym ryzyko agresji podprogowych, działania w cyberprzestrzeni, znaczenie kosmosu, nowe technologie bezzałogowe, zautomatyzowane i wysoce zinformatyzowane systemy walki i wsparcia, sztuczna inteligencja, ryzyka wykorzystywania taktycznej broni jądrowej do tzw. deeskalacji konfliktu konwencjonalnego czy wreszcie zagrożenia pandemiczne.

Strategia z 2020 r. niewiele uwagi poświęca identyfikacji **interesów narodowych.** W zasadzie nie wiadomo, skąd one się biorą i na jakiej podstawie zostały określone. W poprzedniej strategii z 2014 r. interesy narodowe w zakresie bezpieczeństwa jednoznacznie wyprowadzono z Konstytucji RP, opierając na niej ich zdefiniowanie i typologię. Chociaż w obecnej strategii spotyka się podobny opis interesów, to jednak o Konstytucji RP nie ma żadnej wzmianki. Sprawia to wrażenie arbitralnego zdefiniowania najważniejszej kategorii strategii bezpieczeństwa narodowego, jaką są interesy narodowe. Jest to poważny mankament tego dokumentu. Poprzednie strategie

odzwierciedlały logikę czteroetapowego cyklu strategicznego w państwie samodzielnym w swoich decyzjach politycznych:

- identyfikacja interesów narodowych jako punkt wyjścia analiz;
- ocena i prognoza środowiska bezpieczeństwa (dla określenia tego, co może przeszkadzać, a co może pomagać w realizacji tych interesów);
- określenie strategii operacyjnej, czyli sposobów zapewnienia realizacji interesów narodowych w konkretnych warunkach środowiska bezpieczeństwa;
- określenie strategii preparacyjnej, czyli sposobów przygotowania własnego systemu bezpieczeństwa do realizacji wcześniej określonych zadań operacyjnych.

Zdaniem prof. Stanisława Kozieja *Strategia 2020* wydaje się pozbawiona funkcji organizacyjnej, przygotowawczej i funkcjonalnej systemu bezpieczeństwa narodowego w czasie pokoju, zagrożenia i wojny zgodnie z własnymi interesami narodowymi i stosownie do istniejących warunków.

Istotnym i chyba najważniejszym mankamentem obecnej strategii bezpieczeństwa jest całkowity brak strategii operacyjnej, tj. celów i zadań strategicznych dotyczących sposobów przeciwdziałania zagrożeniom (w tym wojennym) i ryzykom, podejmowania wyzwań czy też wykorzystywania szans dla bezpieczeństwa Polski stwarzanych przez środowisko strategiczne. Jej treść można podzielić na dwie części: diagnostyczną i zadaniową. Ta druga składa się z czterech filarów, które dotyczą: bezpieczeństwa państwa i obywateli, Polski w systemie bezpieczeństwa międzynarodowego, tożsamości i dziedzictwa narodowego, rozwoju społeczno-gospodarczego.

W *Białej Księdze Bezpieczeństwa Narodowego RP*[701] z 2015 r. zaproponowano schemat struktury bezpieczeństwa narodowego RP, wyodrębniając dziedziny bezpieczeństwa narodowego traktowane jako sfery aktywności państwa w obszarze bezpieczeństwa, do których zalicza się m.in. obronność, ochronę, bezpieczeństwo społeczne oraz gospodarcze. W przypadku obronności podział dotyczy głównie bezpieczeństwa militarnego i obrony narodowej.

Kolejny dokument, jakim jest *Strategia Bezpieczeństwa* z 9 kwietnia 2013 r., szczególny nacisk kładzie na informacyjność (powszechność informacji wpływa na nastroje i wywołuje presję opinii publicznej na określone działania), asymetryczność (w doborze sił i środków), usieciowienie (sieć instytucji międzynarodowych i narodowych odpowiedzialnych za bezpieczeństwo), zintegrowanie (postępująca integracja wysiłków cywilno-wojskowych). Nowa jakość bezpieczeństwa będzie się przejawiać w takich cechach, jak kompleksowość oraz wieloaspektowość bezpieczeństwa Polski – państwa jako instytucji oraz jego obywateli – co ma wymagać ścisłej integracji jego podstawowych dziedzin (bezpieczeństwo zewnętrzne, polityczne, militarne, ekonomiczne, społeczne, ekologiczne itd.), a także rosnącego powiązania go z rozwojem gospodarczo-społecznym państwa.

Na tle państw unijnych Polska znajduje się na początku budowy zintegrowanego systemu bezpieczeństwa cyberprzestrzeni. Jednym z jego elementów jest przyjęta przez Komitet Stały Rady Ministrów 25 czerwca 2013 r. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej[702]. Zawiera ona koncepcję systemu zarządzania cyberprzestrzenią oraz definiuje zależności między poszczególnymi organami i instytucjami państwowymi, a także ich wyspecjalizowanymi komórkami odpowiedzialnymi za zapewnienie odpowiedniego poziomu bezpieczeństwa teleinformatycznego w cyberprzestrzeni. Nie jest to jednak dokument o charakterze transsektorowym, a jedynie rządowym[703].

Polityka Ochrony Cyberprzestrzeni jako cel strategiczny wskazuje osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa. Jego realizacja powinna się odbywać poprzez stworzenie ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji między użytkownikami cyberprzestrzeni Rzeczypospolitej Polskiej. Do celów szczegółowych natomiast zalicza się zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej[704] państwa, zwiększenie zdolności do zapobiegania i zwalczania zagrożeń w cyberprzestrzeni, ograniczanie skutków incydentów godzących w bezpieczeństwo teleinformatyczne, jednoznaczne określenie kompetencji podmiotów

odpowiedzialnych za bezpieczeństwo w cyberprzestrzeni, stworzenie i realizację spójnego systemu zarządzania bezpieczeństwem w cyberprzestrzeni[705], stworzenie trwałego systemu koordynacji i wymiany informacji między podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz użytkownikami cyberprzestrzeni, a także zwiększenie świadomości użytkowników cyberprzestrzeni w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni.

W tym dokumencie m.in. wskazano, że w obliczu wielu coraz częściej występujących zagrożeń niezbędne jest skoordynowanie działań, które umożliwią szybkie i efektywne reagowanie na ataki wymierzone przeciwko systemom teleinformatycznym i oferowanym przez nie usługom. Systemy teleinformatyczne eksploatowane przez administrację zarówno rządową, jak i samorządową, organy władzy ustawodawczej, władzę sądowniczą, a także systemy strategiczne z punktu widzenia bezpieczeństwa państwa, jak również przedsiębiorcy oraz osoby fizyczne zostały objęte *Polityką Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*[706]. To właśnie w tym dokumencie rząd Rzeczypospolitej Polskiej potwierdził jednoznacznie, że bierze czynny udział w zapewnieniu bezpieczeństwa zasobów informacyjnych państwa, jego obywateli, realizując tym samym swoje konstytucyjne obowiązki.

Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej[707], zwana dalej doktryną, była dokumentem opublikowanym przez Biuro Bezpieczeństwa Narodowego i stanowiła podstawę koncepcyjną do przygotowania oraz realizacji skoordynowanych w skali państwa działań poszczególnych podmiotów z sektora publicznego i prywatnego na rzecz cyberbezpieczeństwa RP. Dokument ten nie stanowił podstawy prawnej, był natomiast transsektorowym dokumentem wykonawczym do *Strategii Bezpieczeństwa Narodowego RP*. Prawne ujęcie cyberprzestrzeni pozwalało zaobserwować, że pojęcie to dopiero zakorzenia się w prawie polskim i z czasem stanie się pojęciem potocznie używanym w wymiarze sprawiedliwości.

Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej zaprezentowana 22 stycznia 2015 r. określała warunki do zespolenia i

strategicznego ukierunkowania wysiłków na rzecz budowania zintegrowanego systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej[708]. Precyzowała cel strategiczny, który można osiągnąć przez realizację zadań o charakterze operacyjnym i przygotowawczym w dziedzinie cyberbezpieczeństwa. Zawierała ocenę zagrożeń, ryzyk i szans w dynamicznie rozwijającym się środowisku cyberbezpieczeństwa (w jego wymiarze zewnętrznym i wewnętrznym, krajowym i międzynarodowym), identyfikowała najważniejsze zadania operacyjne dla zapewnienia cyberbezpieczeństwa w sektorze publicznym, prywatnym i obywatelskim oraz rekomendowała zadania preparacyjne mające na celu doskonalenie, rozwój i transformację systemu cyberbezpieczeństwa, z uwzględnieniem podsystemu kierowania oraz publicznych i prywatnych ogniw wykonawczych[709]. Dokument został przygotowany w wyniku analiz prowadzonych z udziałem przedstawicieli administracji publicznej, środowiska akademickiego, organizacji pozarządowych oraz sektora prywatnego. Główne założenia zostały rozpatrzone i zaakceptowane przez Radę Bezpieczeństwa Narodowego. Doktryna wskazuje strategiczne kierunki działań dla zapewnienia pożądanego poziomu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni. Powinna być jednocześnie traktowana jako jednolita podstawa koncepcyjna zapewniająca spójne i kompleksowe podejście do zagadnień cyberochrony i cyberobrony – jako wspólny mianownik działań realizowanych przez podmioty administracji publicznej, służby bezpieczeństwa i porządku publicznego, siły zbrojne, sektor prywatny oraz obywateli[710]. Dzięki temu mogła stanowić punkt wyjścia do dalszych prac nad rzecz wzmocnienia bezpieczeństwa Polski i Polaków w cyberprzestrzeni[711].

W kwietniu 2017 r. uchwałą nr 52/2017 Rady Ministrów przyjęto dokument strategiczny dotyczący bezpieczeństwa cyberprzestrzeni w postaci *Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022* (dalej Krajowe Ramy). Powstał on w efekcie prac zespołu międzyresortowego pod kierunkiem Ministerstwa Cyfryzacji[712]. Stanowił kontynuację działań zapoczątkowanych w programie ochrony cyberprzestrzeni na lata 2011–2016[713]. Jednym z podstawowych zadań wskazanych w Krajowych Ramach jest uzyskanie

wysokiego poziomu odporności krajowych systemów teleinformatycznych służących świadczeniu usług kluczowych, usług cyfrowych oraz usług administracji publicznej. W tym celu przewidziano rozbudowę krajowego systemu cyberbezpieczeństwa w taki sposób, aby był ukierunkowany na uzyskanie zdolności w zakresie bieżącego monitorowania zagrożeń oraz zintegrowanego zarządzania cyberbezpieczeństwem w skali państwa.

Działania te podjęte przez Ministerstwo Cyfryzacji we współpracy z innymi resortami wynikają ze zmiany ustawy z dnia 4 września 1997 r. o działach administracji rządowej[714] w grudniu 2015 r.[715], która przypisała do działu „informatyzacja" kompetencje w zakresie bezpieczeństwa cyberprzestrzeni. Działania są motywowane potrzebą ustanowienia kompleksowego systemu bezpieczeństwa teleinformatycznego państwa. Zalecenie to zostało sformułowane w związku z kontrolą przeprowadzoną przez Najwyższą Izbę Kontroli w 2014 r. w instytucjach publicznych odpowiedzialnych za bezpieczeństwo cyberprzestrzeni.

22 października 2019 r. Rada Ministrów przyjęła uchwałę nr 125 w sprawie *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*[716]. Dokument obowiązuje od 31 października 2019 r. i zastępuje *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*. Przyjęcie strategii wynika z art. 68 ustawy o krajowym systemie cyberbezpieczeństwa z 5 lipca 2018 r.

Strategia z 2019 r. jest bardzo podobna do wcześniejszej i jej ram przyjętych w maju 2017 r. Jest jednak pierwszą krajową strategią w zakresie bezpieczeństwa systemów teleinformatycznych, stąd jej głównym celem przyjęcia i wdrożenia jest podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach publicznym, militarnym i prywatnym, a także promowanie dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.

Uchwalenie nowej strategii wynikało z art. 68 i n. ustawy o krajowym systemie cyberbezpieczeństwa. Ponadto w raporcie NIK[717] stwierdzono, że „istotnym czynnikiem wpływającym negatywnie na realizację zadań w obszarze bezpieczeństwa w cyberprzestrzeni było niewystarczające zaangażowanie kierownictwa administracji

rządowej, w tym Prezesa Rady Ministrów […] a także, że znaczącym osłabieniem poziomu cyberbezpieczeństwa jest fakt, że poszczególne kontrolowane podmioty posiadały własne, odrębne procedury zapobiegania zagrożeniom w cyberprzestrzeni, jednak nie tworzyły one jednego spójnego systemu".

Strategia została uchwalana na 5 lat, a koordynatorem jej wdrażania jest minister właściwy ds. informatyzacji. Po dwóch latach dokument podlega przeglądowi i aktualizacji. Określono *Krajowe Ramy Strategii* jako dokument, „który wpisuje się w kontynuację działań, podejmowanych w przeszłości przez administrację rządową, mających na celu podniesienie poziomu bezpieczeństwa w cyberprzestrzeni RP do 2022 r. Ich celem jest określenie ramowych działań zmierzających do uzyskania wysokiego poziomu odporności krajowych systemów teleinformatycznych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty w cyberprzestrzeni. Proponowane kierunki strategiczne mają również wpływać na zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu przestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni. *Krajowe Ramy Polityki Cyberbezpieczeństwa* są spójne z prowadzonymi działaniami dotyczącymi operatorów infrastruktury krytycznej wykorzystujących systemy teleinformatyczne oraz uwzględnia potrzeby zaangażowania Sił Zbrojnych Rzeczypospolitej[718].

Wyznacza pięć celów szczegółowych polityki rządu w tym zakresie:

- rozwój krajowego systemu cyberbezpieczeństwa;
- podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania incydentom i reagowania na nie;
- zwiększanie potencjału narodowego w kwestii bezpieczeństwa w cyberprzestrzeni;
- budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa;
- zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

Oznacza to, że rząd przewiduje aktualizację ustawy o krajowym systemie cyberbezpieczeństwa na podstawie doświadczeń wynikających z jej wdrażania. Bardzo ważnym elementem będzie także wypracowanie i wdrożenie metodyki szacowania ryzyka, co pozwoli na odpowiednie zarządzanie ryzykiem w skali kraju. To duże przedsięwzięcie organizacyjne, ponieważ do tej pory analiza ryzyka nie była spójna. Taki cel pojawił się już w Krajowych Ramach, jednak nie udało się go zrealizować.

Będzie to związane z opracowaniem i wdrożeniem *Narodowych Standardów Cyberbezpieczeństwa* oraz promowaniem dobrych praktyk i zaleceń, bezpieczeństwa łańcucha dostaw, testów i audytów cyberbezpieczeństwa. Opracowanie standardów ma wpłynąć na zwiększenie odporności systemów teleinformatycznych administracji publicznej. Przewidziane są prace nad standardami dotyczących aplikacji, urządzeń mobilnych oraz serwerów i sieci. W tym aspekcie istotne jest także wdrożenie aktu o cyberbezpieczeństwie[719], wprowadzającego certyfikację produktów i usług ICT. W Polsce musi zostać utworzony krajowy system oceny i certyfikacji w zakresie cyberbezpieczeństwa, m.in. powołanie lub ustanowienie Krajowego Organu ds. Certyfikacji Cyberbezpieczeństwa (KOCC), krajowej jednostki akredytującej oraz jednostek oceniających zgodność.

Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa obejmuje rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa, nastawienie na rozwój współpracy między sektorami publicznym i prywatnym, stymulowanie badań i rozwoju w obszarze cyberbezpieczeństwa, a także uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni. Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa dotyczy zwiększania kompetencji kadry podmiotów istotnych dla cyberbezpieczeństwa Rzeczypospolitej Polskiej, stworzenia warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli oraz rozwijania świadomości społecznej w kierunku bezpiecznego korzystania z cyberprzestrzeni.

Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa ma polegać na tym, że rząd

będzie prowadził aktywną współpracą międzynarodową na poziomach strategiczno-politycznym oraz operacyjnym i technicznym. Działania te są istotne wobec planowanej nowelizacji dyrektywy NIS oraz uznania przez NATO cyberprzestrzeni za domenę działań operacyjnych.

Jego celem była implementacja dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r.[720] w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii zwanej dalej dyrektywą NIS[721]. Dopiero wejście w życie dyrektywy NIS doprecyzowało to pojęcie. Ponadto problematyka prawna cyberprzestrzeni nie była i nie jest wystarczająco uregulowana w skali globalnej[722]. O ile w państwach Unii Europejskiej są dokumenty w pewnym stopniu regulujące incydenty w cyberprzestrzeni, to nie istnieją żadne normy ujmujące prawnie cyberprzestrzeń w skali światowej, których przestrzeganie byłyby egzekwowane. W innych dokumentach tego typu można znaleźć opisane obszary bezpieczeństwa państwa obejmujące problematyką różne podmioty, dziedziny i sektory bezpieczeństwa narodowego, w tym cyberbezpieczeństwo. W tym przypadku najpoważniejszym zagrożeniem jest cyberterroryzm definiowany jako „przemyślany politycznie lub niemilitarnie motywowany atak albo groźba ataku na systemy teleinformatyczne celem sparaliżowania lub poważnego zniszczenia Infrastruktury Krytycznej Państwa oraz zastraszenia i wymuszenia na rządzie lub społeczności daleko idących polityczno-militarnych działań”[723].

Zapewnienie bezpieczeństwa informacji jest wyzwaniem dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa, a więc podmiotów gospodarczych świadczących usługi przy wykorzystaniu systemów teleinformatycznych, użytkowników cyberprzestrzeni, organów władzy publicznej, a także wyspecjalizowanych podmiotów zajmujących się bezpieczeństwem teleinformatycznym w sferze operacyjnej. Jest to tym istotniejsze, że Polska jest ściśle powiązana z innymi państwami przez współpracę międzynarodową w ramach takich organizacji, jak UE, NATO, ONZ czy OBWE[724]. Współpraca ta odgrywa istotną rolę w walce z rosnącą liczbą

incydentów powodowanych nielegalnymi działaniami w cyberprzestrzeni prowadzącymi do strat materialnych i wizerunkowych.

Główne założenia obecnej strategii zostały skierowane na[725]:

- potrzebę zapobiegania i reagowania w odniesieniu do incydentów oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa;
- zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych.

Ponadto zostały też wyodrębnione cztery cele szczegółowe wskazujące na potrzeby wynikające z rozbudowy krajowego systemu cyberbezpieczeństwa:

- stworzenie zasad dobrej współpracy między sektorami publicznym i prywatnym oraz umiejętne podejście do oceny ryzyka wystąpienia ataku w cyberprzestrzeni;
- edukację, informację i szkolenia dotyczące cyberbezpieczeństwa;
- działania odnoszące się do planów badawczo-rozwojowych w zakresie bezpieczeństwa teleinformatycznego;
- współpracę międzynarodową w zakresie cyberbezpieczeństwa.

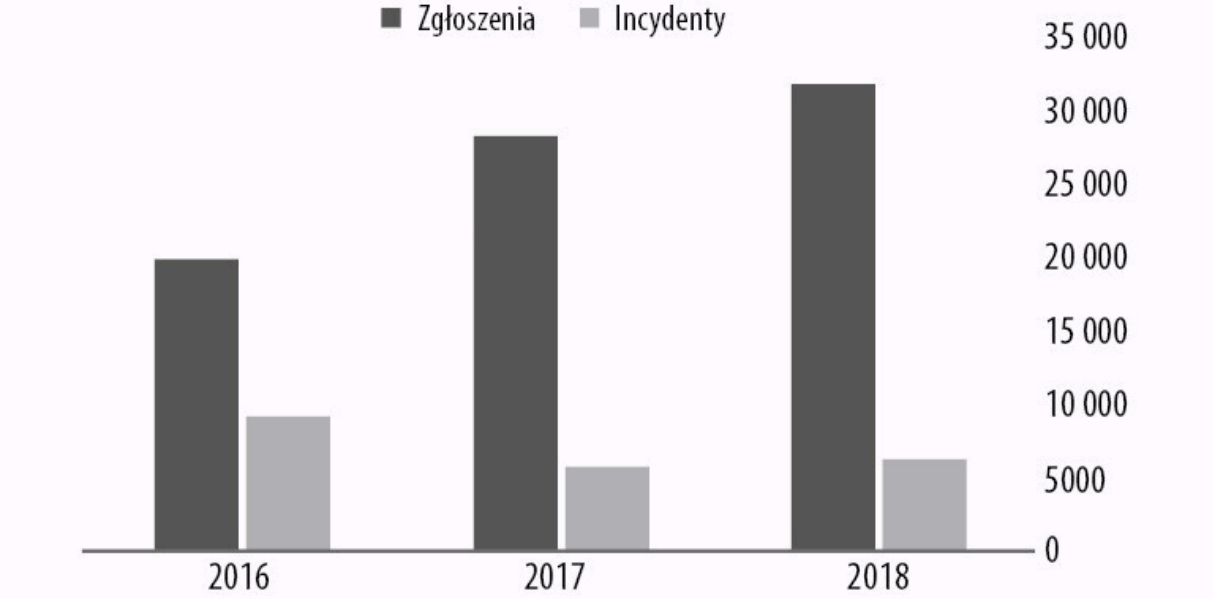
Realizacja tych celów jest związana ze zmianami prawnymi oraz udoskonaleniem struktury systemu cyberbezpieczeństwa przez jasny podział kompetencji, który zwiększyłby efektywność współdziałania podmiotów odpowiedzialnych za bezpieczeństwo sieci. będzie się to wiązać również ze stworzeniem i wdrożeniem systemu zarządzania ryzykiem teleinformatycznym w skali państwa[726]. Duży nacisk został położony na ochronę infrastruktury krytycznej usług kluczowych i cyfrowych, zwalczanie cyberprzestępczości i cyberterroryzmu, a także uzyskania zdolności do prowadzenia szeroko zakrojonych działań militarnych w cyberprzestrzeni. Ważnym elementem dokumentu jest także budowanie kompetencji w zakresie cyberbezpieczeństwa – rozbudowa zasobów przemysłowych i technologicznych, budowanie

partnerstw publiczno-prywatnych, stymulowanie badań i rozwoju, a także edukacja w zakresie cyberbezpieczeństwa[727].

Za pośrednictwem cyberprzestrzeni złośliwy kod może być natychmiast rozmieszczony z dowolnego miejscu na świecie[728]. Dokładna identyfikacja osób odpowiedzialnych za cyberataki oraz reagowanie na szkodliwe działania, a nawet zapobieganie im wydają się znacznie trudniejsze w cyberprzestrzeni niż w świecie realnym. Można przypuszczać, że incydenty i spory toczące się w cyberprzestrzeni będą się nasilać, stając się jednym z głównych zagrożeń bezpieczeństwa państwa. Cybernarzędzia dają możliwość nękania wroga i demonstrowania własnych możliwości, mogą być także pewnego rodzaju narzędziem nacisku na przeciwną stronę. Kluczową rolę odgrywają jednak władze określonego państwa, które inicjują cyberzagrożenia oraz je interpretują. Jeśli cyberataki są powszechnie widoczne i odczuwalne przez społeczeństwo, to ich konsekwencje zmuszają do zajęcia stanowiska i zdecydowanego działania przez władze państwa, które stały się ofiarą tych szkodliwych działań. Przypadek Polski jest nieco inny w porównaniu z wydarzeniami choćby w Estonii z 2007 r.[729] Polska nie została doświadczona w takiej skali, o czym świadczą wyniki badań ilustrujące poziom rozwoju ICT. O tym, że serwis internetowy KNF był od 5 października 2016 r. zainfekowany złośliwym oprogramowaniem i o szkodliwości cyberataku, jego administratorzy dowiedzieli się podobnie, jak to miało miejsce w Tallinie. Dlatego też, jak można sądzić, intensywność inicjatyw w zakresie polityki bezpieczeństwa cybernetycznego w przypadku tych państw pozostaje na innym stopniu zaawansowania, o czym można było się dowiedzieć z mediów na początku lutego 2017 r., gdy kolejne banki poinformowały opinię publiczną, że padły ofiarą cyberataku, nieświadomie pobrawszy złośliwe oprogramowanie z serwisu informacyjnego Komisji Nadzoru Finansowego[730]. Atak na taką skalę z pewnością by się nie powiódł, gdyby na poziomie zarówno zarządzania systemami informatycznymi polskiego regulatora finansowego, jak i ochrony sprzętowej i sieciowej banków oraz instytucji finansowych zachowano przynajmniej minimalne standardy ostrożności, które wymagałyby przede wszystkim bieżącej aktualizacji oprogramowania oraz ciągłego

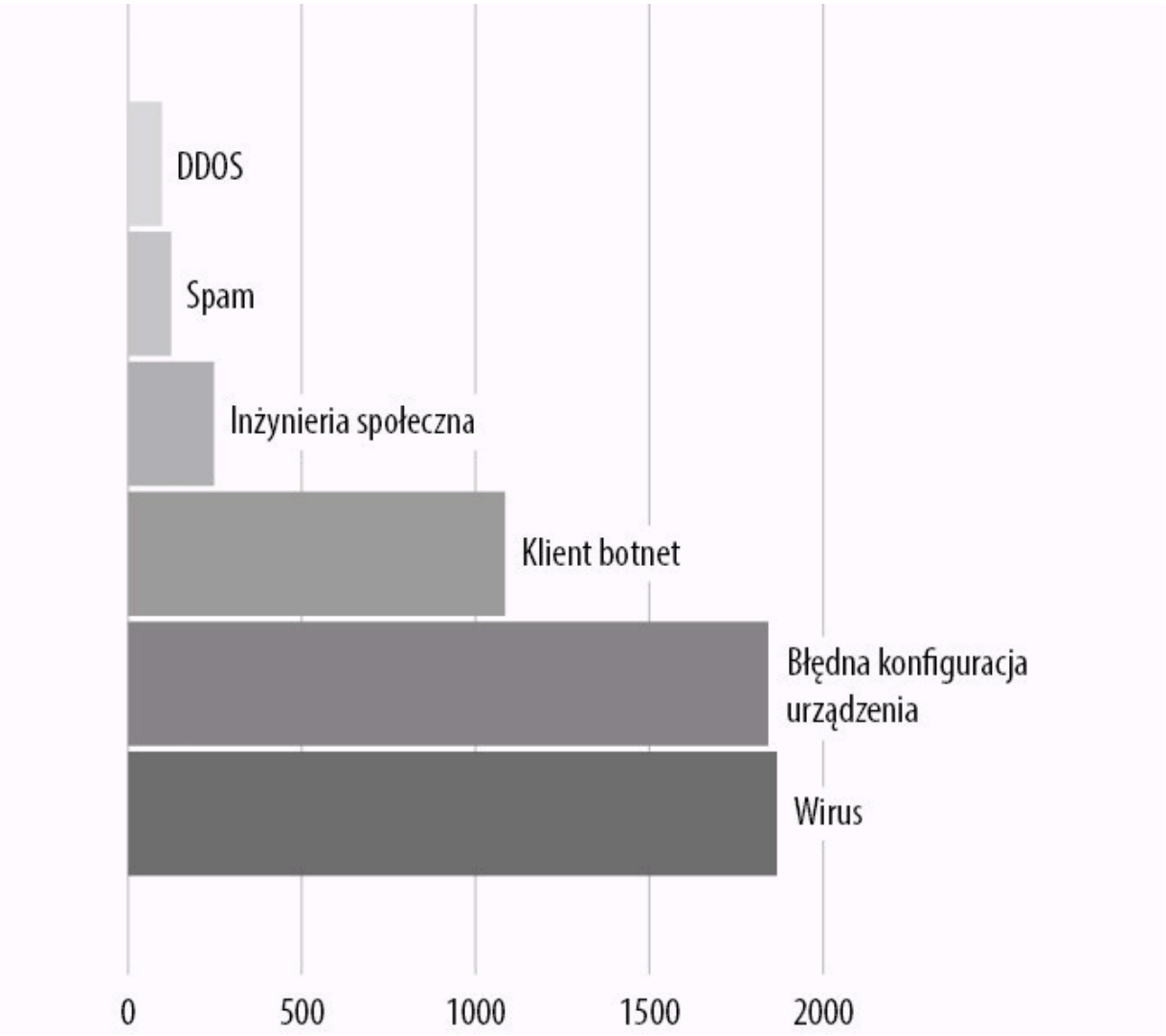
monitorowania ruchu sieciowego z infrastruktury zawierającej informacje chronione.

Wzrost zainteresowania potencjalnych atakujących sieci w Polsce oraz stosunkowy wzrost incydentów jest wynikiem błędnych konfiguracji albo braku aktualizacji programów komputerowych. Różnica zgłoszeń incydentów w poszczególnych latach wynikała m.in. z zasięgu i intensywności kampanii phishingowych, propagacji złośliwego oprogramowania oraz podjętych działań przez jednostki administracji publicznej w stosunku do zgłoszeń dotyczących w szczególności błędnych konfiguracji urządzeń oraz klientów sieci botnet[731].



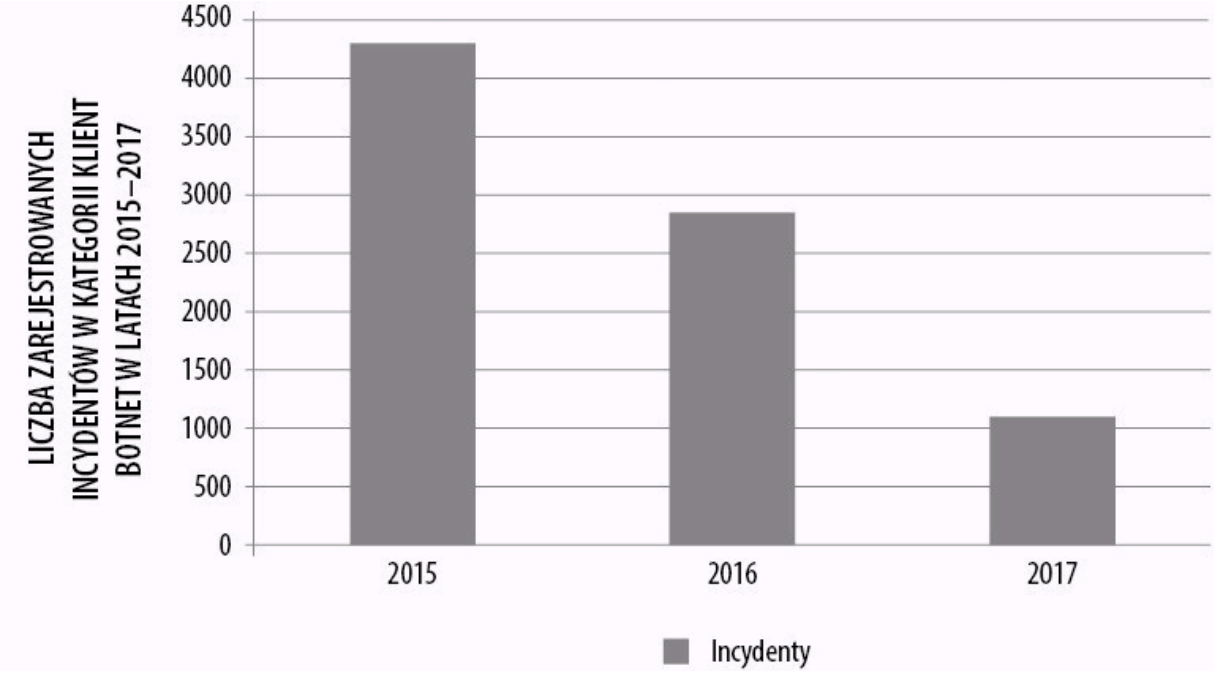
RYSUNEK 6.2 Analiza zgłoszeń i incydentów w latach 2016–2018 w Polsce

Źródło: Opracowanie własne na podstawie danych z Raportu csirt.gov.pl (dostęp: 27.05.2020).



RYSUNEK 6.3 Źródła zgłoszeń incydentów w Polsce

Źródło: Opracowanie własne na podstawie danych z Raportu csirt.gov.pl (dostęp: 27.05.2020).



RYSUNEK 6.4
Liczba zarejestrowanych incydentów w kategorii klient botnet w latach 2015–2017

Źródło: Opracowanie własne na podstawie danych z Raportu csirt.gov.pl (dostęp: 27.05.2019).

Po okresie spokoju charakteryzującego koniec 2017 r. nastąpił powrót długotrwałych ataków: najdłuższy trwał 297 godzin (12,4 dni), choć nie był to rekord światowy. Dłuższy atak miał miejsce pod koniec 2015 r. Występowanie innych długotrwałych ataków (co najmniej 50 godzin) zwiększyło się ponad sześciokrotnie, z 0,10 do 0,63%. Odnotowano również występowanie najkrótszych ataków (do 9 godzin) – o ile w zeszłym kwartale stanowiły one 85,5% wszystkich ataków, obecnie stanowią 91,47%. Z kolei liczba ataków trwających od 10 godzin do trzech dni zmniejszyła się niemal o połowę, z 14,85 do 7,76%.

Kolejnym istotnym zagadnieniem jest rodzaj odnotowywanych incydentów. W 2017 r. najczęściej występujące zdarzenia należały do kategorii *wirus,* definiowanej jako uzyskanie informacji na temat prawdopodobnej infekcji stacji roboczej, serwerów lub urządzeń sieciowych. Cyberprzestępcy bardzo często wykorzystują elementy inżynierii społecznej (np. złośliwe załączniki w wiadomościach e-

mail) w celu propagacji złośliwego oprogramowania. Takie wiadomości zaklasyfikowano do kategorii *wirus*.

Drugą najczęściej występującą kategorią w 2017 r. była błędna konfiguracja urządzenia, odnotowano 1847 takich incydentów. Należy podkreślić, że ten rodzaj zagrożenia bezpieczeństwa, choć nie wynika z ingerencji zewnętrznej w system, w wielu przypadkach może stanowić furtkę do przeprowadzenia skutecznego ataku.

Incydenty z trzeciej najczęściej występującej kategorii – klient sieci botnet – to zdarzenia, w których za pomocą systemów wspomagających zaobserwowano próby połączenia (bardzo często udane) stacji roboczych z adresami, domenami sklasyfikowanymi jako serwery C&C, lub charakterystyka ruchu sieciowego odpowiadała wskaźnikom IoC znanych sieci botnet. Mimo że nadal incydenty tej kategorii znajdują się na trzecim miejscu, w od 2017 r. odnotowano wyraźną tendencję spadkową w tym zakresie. Wynika to m.in. z prowadzonych na całym świecie działań przeciwko systemom kierującym grupami zarażonych komputerów, czyli tzw. serwerami C&C[732].

6.2.2. POLSKI KODEKS KARNY WOBEC POLITYKI CYBERBEZPIECZEŃSTWA

W *Kodeksie karnym* do tej kategorii przestępstw będzie można zaliczyć przestępstwa terrorystyczne z rozdziału XXXIII k.k.[733]: przestępstwa przeciwko ochronie informacji, a w szczególności cyberprzestępstwa z art. 268 i 268a k.k. oraz art. 269 i 269a k.k. jako typ kwalifikowany przestępstw. Do tej kategorii terroryzmu można zakwalifikować przestępstwo przeciwko bezpieczeństwu powszechnemu z art. 165 § 1 pkt 4 k.k., polegające na sprowadzeniu niebezpieczeństwa dla życia lub zdrowia wielu osób albo mienia w znacznych rozmiarach, które jest następstwem zakłócania, uniemożliwiania lub wpływania w inny sposób na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych. Cechą tego przestępstwa jest sprowadzenie niebezpieczeństwa narastającego w czasie, które ponadto musi być realne i konkretne, ustawodawca nie wymaga natomiast, aby sprowadzone niebezpieczeństwo było bezpośrednie.

Pojęcie zakłócenia automatycznego przetwarzania, przekazywania lub gromadzenia danych informatycznych obejmuje wszelkie czynności oddziałujące na te procesy, których skutkiem jest ich nieprawidłowy przebieg lub spowolnienie, a także zniekształcenie czy modyfikacja przetwarzanych, przekazywanych lub gromadzonych danych informacji. Natomiast „uniemożliwienie" oznacza zatrzymanie tych procesów lub niemożność ich podjęcia. Zdaniem A. Marka[734] wymaganie, aby przestępstwo skutkowo określone w art. 165 § 4 k.k. stworzyło konkretne zagrożenie życia lub zdrowia wielu osób albo mienia w wielkich rozmiarach, chyba nadmiernie ogranicza możliwość penalizacji.

Przestępstwo z art. 267 § 1 k.k. (hakerstwo)[735] jest przestępstwem powszechnym, a jego sprawcą we wszystkich odmianach może być wyłącznie osoba, która sama nie jest uprawniona do uzyskania określonej informacji, a w szczególności nie jest jej dysponentem. Czyn zabroniony z art. 267 § 1 k.k. może zostać popełniony z zamiarem bezpośrednim lub ewentualnym. Potwierdził to Sąd Najwyższy[736], który podkreślił, że wprawdzie przepis art. 267 § 1 k.k. nie zawiera charakterystycznego zwrotu, który redukowałby w stronie podmiotowej umyślność do zamiaru bezpośredniego, to jednak cała konstrukcja tego typu przestępstwa, a w szczególności znamię czasownikowe „uzyskuje"[737] i znamiona określające bliżej sposób owego uzyskania, eliminują w istocie możliwość popełnienia tego występku w zamiarze wynikowym.

Nowelizacja *Kodeksu karnego* z 2004 r. przeprowadzona w celu dostosowania polskich przepisów karnych do wymagań europejskich wprowadziła znacznie ograniczoną karalność uzyskania nieuprawnionego dostępu do systemu informatycznego. Owe mankamenty przepisu 267 1 k.k. zostały usunięte nowelą *Kodeksu karnego* z września 2008 r., której celem była m.in. implementacja do polskiego porządku prawnego decyzji ramowej Rady 2005/222/WSiSW[738] w sprawie ataków na systemy informatyczne. Wspomniana nowelizacja zmieniła treść art. 267 § 1 k.k. przez zastąpienie sformułowania „uzyskuje informację dla niego nieprzeznaczoną" nowym sformułowaniem „uzyskuje dostęp do informacji dla niego nieprzeznaczonej".

Warto zaznaczyć, że obecne brzmienie art. 267 § 1 k.k. nie wskazuje, w jaki sposób ma się odbyć podłączenie do sieci. Takie podejście wydaje się trafne, gdyż podłączenie to może odbywać się na wiele sposobów. Również w tym przypadku zmiana poszerza zakres penalizacji omawianego przepisu i z pewnością go racjonalizuje.

Kolejna ze wskazanych zmian art. 267 § 1 k.k. polega na dodaniu obok „przełamania" kolejnej czynności w postaci „ominięcia" zabezpieczenia sieci telekomunikacyjnej. Jak zaznaczył R. Zawłocki[739], czynność polegająca na „przełamaniu" zabezpieczenia sieci telekomunikacyjnej nie odnosiła się do „fizycznego" aspektu tej czynności, lecz nawiązywała do jej abstrakcyjnego potocznego ujęcia. Sprawca „przełamywał" zabezpieczenia w ten sposób, że je w różny sposób pokonywał. Wprowadzenie nowej czynności sprawia, że dotychczasowe ujęcie „przełamania" należy ujmować nieco odmiennie, a ściślej – jest zawężone. Wydaje się bowiem, że w obecnym stanie prawnym „przełamanie" będzie się odnosiło do czynności bezpośrednio ingerującej w system zabezpieczeń, gdy tymczasem „ominięcie" będzie polegało na pokonaniu zabezpieczenia bez takiej ingerencji.

Zgodnie z art. 7 decyzji ramowej przestępstwo hakerstwa poprzedzone przełamaniem szczególnych zabezpieczeń, jeżeli zostało popełnione w zorganizowanej grupie przestępczej, powinno być zagrożone karą pozbawienia wolności co najmniej od 2 do 5 lat. *Kodeks karny* nie przewiduje natomiast zaostrzenia kary za to przestępstwo w takiej sytuacji. W tym zakresie art. 267 k.k. jest więc niezgodny z art. 7 decyzji. Z uwagi na to, że analogiczne rozwiązanie zostało przyjęte w art. 2 konwencji o cyberprzestępczości[740], art. 267 k.k. jest niezgodny także z konwencją.

Ustawa z października 2008 r. zmieniającą ustawę Kodeks karny dodała w art. 267 § 2 k.k. nowy typ czynu zabronionego, a mianowicie nieuprawniony dostęp do systemu komputerowego. Zgodnie z treścią tego przepisu: „karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego". Do tej pory czyn ten nie był kryminalizowany, co z pewnością można było uznać za istotną lukę. Jeżeli bowiem penalizowany jest nieuprawniony dostęp do informacji, to tym bardziej powinien być zabroniony dostęp do

systemu informatycznego bądź jego części. Jak zauważają twórcy wspomnianej nowelizacji, nowy art. 267 § 2 k.k. ustanawia karalność czynu, którego skutkiem jest uzyskanie bez uprawnienia, dostępu do systemu informatycznego lub jego części, nawet bez złamania jakiegokolwiek zabezpieczenia zainstalowanego w komputerze użytkownika lub zabezpieczenia systemowego. Przykładem takiego czynu może być wprowadzenie do systemu informatycznego oprogramowania, które umożliwia sprawcy przejęcie zdalnej kontroli nad komputerem w celu wykonania z jego wykorzystaniem zmasowanych ataków na określone strony internetowe. W takim przypadku sprawca nie działa w celu uzyskania informacji znajdującej się w zasobach przejętego systemu lub dostępu do niej, lecz w celu przejęcia kontroli nad systemem jako narzędziem do bezprawnego wykorzystywania. Przewidując omawiany nowy typ przestępstwa, projekt usuwa istotną lukę w obowiązującym prawie, gdyż tego rodzaju szkodliwe działania pozostają obecnie poza zakresem penalizacji.

Przepisem, który najpełniej sankcjonuje naruszenie zakazu posługiwania się specjalistycznym oprogramowaniem instalowanym w systemach informatycznych bez wiedzy ich dysponentów (w szczególności oprogramowaniem typu *spyware*), jest art. 267 § 3 k.k.[741] Zgodnie z tym przepisem zabronione jest zakładanie lub posługiwanie się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem w celu uzyskania informacji, do której sprawca jest nieuprawniony. Jak podkreśla A. Adamski, w odróżnieniu od art. 267 § 1 k.k. karalność zachowania określonego w § 3 opiera się na bardziej zobiektywizowanym kryterium karalności, jakim jest zakładanie urządzeń technicznych lub posługiwanie się nimi w celu uzyskania zastrzeżonych informacji. Przepis ten nie uzależnia karalności przechwycenia informacji od przełamywania przez sprawcę żadnych szczególnych postaci zabezpieczeń. Dla realizacji znamion strony podmiotowej niezbędne jest natomiast działanie w celu uzyskania informacji, do których sprawca czynu nie jest uprawniony.

Zasadnicze znaczenie dla określenia przypadków, w których działalność hakerów będzie wypełniać znamiona typu czynu zabronionego z art. 267 § 3 k.k., ma ustalenie, jak z punktu widzenia

specyfiki działalności wykorzystującej techniki informatyczne należy rozumieć pojęcie „urządzenia", którym posługuje się ten przepis. Za urządzenie z pewnością nie można uznać programu komputerowego, gdyż jest on rozumiany jako zestaw instrukcji (rozkazów) napisany w języku zrozumiałym dla urządzenia, jakim jest np. komputer, i bez jego udziału nie jest zdolny do wykonywania żadnych czynności. W tym przypadku za urządzenie możemy uznać system komputerowy, na którym zostało zainstalowane specjalistyczne oprogramowanie służące do uzyskiwania informacji chronionych. Z punktu widzenia prawa nie ma istotnego znaczenia, czy sprawca wykorzystuje program zainstalowany na własnym komputerze (narzędzie ataku), czy też komputerze stanowiącym obiekt ataku.

Analizując zgodność art. 267 § 3 k.k. z prawem europejskim, należy zaznaczyć, że odpowiada on pod względem penalizowanego zachowania art. 3 konwencji o cyberprzestępczości, decyzja ramowa natomiast nie odnosi się do tego czynu.

Zgodnie z art. 267 § 4 k.k. karze podlega także osoba trzecia, która, wiedząc o tym, że dana informacja została uzyskana w sposób nielegalny, np. przy użyciu urządzeń podsłuchowych, ujawnia taką informację innej osobie. Jedną z form popełnienia tego przestępstwa będzie więc przekazywanie sobie przez hakerów zdobytych w sposób nielegalny informacji o kodach dostępu, „złamanych" hasłach do systemów informatycznych czy też skradzionych numerach kart kredytowych.

Istota określonego w art. 268 § 1 przestępstwa polega na udaremnianiu lub utrudnianiu dostępu do informacji osobie do tego uprawnionej. Penalizowane działanie może polegać na zniszczeniu (tj. całkowitym unicestwieniu), uszkodzeniu (zepsuciu), usunięciu lub zmianie zapisu istotnej informacji. Chodzi tu o ingerencję dotyczącą wszelkich urządzeń lub przedmiotów zawierających zapis informacji (rękopis, tekst wydrukowany w dowolnej formie, płyta DVD, CD itp.). Podmiotem tego przestępstwa może być tylko osoba nieuprawniona do dokonywania ingerencji, która nie dysponuje przedmiotową informacją (przestępstwo indywidualne).

Bezpośrednim przedmiotem ochrony jest w tym przypadku bezpieczeństwo informacji przechowywanych, przesyłanych i

przetwarzanych w systemach informatycznych. Bezpieczeństwo to ma istotne znaczenie dla funkcjonowania gospodarki, w szczególności zakłócenie działania systemów może wywołać zagrożenie dla takich dóbr jak życie, zdrowie, bezpieczeństwo powszechne[742]. Przestępstwo określone w art. 268 k.k. ma charakter przestępstwa powszechnego, jego sprawcą może być wyłącznie osoba, która nie jest uprawniona do uzyskania określonej informacji, w szczególności nie jest jej dysponentem.

Omawiane przestępstwo we wszystkich jego typach (art. 268 § 1–3) wymaga umyślności działania, przy czym czynności takie jak „usuwanie", „zmienianie", „udaremnianie" lub „utrudnianie" wymagają niewątpliwie zamiaru bezpośredniego. Spowodowanie znacznej szkody majątkowej[743], o której mowa w art. 268 § 3, może natomiast być objęte również zamiarem ewentualnym[744]. Ustawa nie używa tutaj określenia „następstwo" czynu, toteż za nieuprawniony trzeba uznać pogląd, że skutek w postaci znacznej szkody majątkowej może być objęty nieumyślnością na podstawie konstrukcji art. 9 § 3.

Jak podkreśla W. Wróbel[745], oceny istotności informacji należy dokonywać według kryteriów obiektywnych, biorąc pod uwagę interesy osoby uprawnionej do zapoznania się z nią. Określona informacja, która dla osoby posiadającej znaczny majątek nie ma istotnego znaczenia, może mieć taki przymiot dla osoby gorzej usytuowanej. Gdy nieuprawniona ingerencja dotyczy zapisu na komputerowym nośniku informacji (np. dysk twardy), *Kodeks karny* przewiduje wyższą sankcję (art. 268 § 2), co wiąże się ze zwiększoną szkodliwością takiego czynu (np. skasowanie zapisów, wprowadzenie do systemu komputerowego wirusa itp.)[746].

Dalsze zaostrzenie karalności wiąże się z wyrządzeniem za pomocą zachowań określonych w art. 268 § 1 lub 2 dysponentowi zapisu informacji znacznej szkody majątkowej (art. 268 § 3). Chodzi tu z pewnością nie tyle o bezpośredni uszczerbek majątkowy (wartość majątkową zniszczonego lub uszkodzonego urządzenia lub zapisu informacji), ile o szkodę, jaką ponosi dysponent informacji w następstwie tego czynu (np. skasowanie zapisów w księgowości może powodować czasochłonne i kosztowne jej odtwarzanie, zniszczenie lub zniekształcenie dzieła autorskiego może pozbawić autora

spodziewanych korzyści związanych z jego sprzedażą). Wielkość szkody nie może być mniejsza niż wskazana w art. 115 § 5 i 7.

Dopełnieniem art. 268 § 2 k.k. ma być art. 268a k.k., w którym zbiorczo ujęto dwa rodzaje zakazanego zachowania się sprawcy. Pierwszym z nich jest niszczenie, uszkadzanie, usuwanie, zmiana oraz utrudnianie dostępu do wszystkich danych informatycznych. Drugi rodzaj zachowania godzi w proces prawidłowego automatycznego przetwarzania, gromadzenia i przekazywania danych informatycznych w stopniu istotnym. Zachowanie to może polegać na zakłócaniu lub uniemożliwianiu działania procesu[747]. Pojęcie zakłócenia automatycznego przetwarzania, przekazywania lub gromadzenia danych informatycznych obejmuje wszelkie czynności oddziałujące na te procesy, których skutkiem jest ich nieprawidłowy przebieg lub spowolnienie, a także zniekształcenie czy modyfikacja przetwarzanych, przekazywanych lub gromadzonych danych informacji. Uniemożliwienie natomiast oznacza zatrzymanie tych procesów lub niemożność ich podjęcia. W przypadku czynu z art. 268a k.k. mówimy o obiektywnym, a nie subiektywnym znaczeniu słowa „istotność".

Kodeks karny nie zawiera definicji pojęcia „dane informatyczne", podobnie jak nie zostało zdefiniowane pojęcie „komputerowy nośnik informacji". Dane informatyczne w rozumieniu art. 268a k.k. oznaczają zatem dowolny ciąg znaków, posiadający funkcjonalne znaczenie w ramach systemu informatycznego, a więc służące przeprowadzeniu określonej operacji w ramach tego systemu.

Przestępstwa z art. 268 § 2 i art. 268a k.k. mają charakter przestępstw skutkowych, co oznacza, że nie każda ingerencja w treść danych będzie podlegała karze. W szczególności nie będzie karalne takie działanie, które polega jedynie na zapoznaniu się z treścią niechronionych informacji[748].

Zamachy na integralność cyfrowego zapisu informacji mogą powodować znaczne szkody nie tylko ze względu na wartość utraconej lub zniszczonej informacji, ale przede wszystkim ze względu na konsekwencje, jakie mogą powodować.

Ustawodawstwo polskie, jako jedno z nielicznych na świecie, przewiduje karalność sabotażu komputerowego rozumianego jako

działanie sprawcy mające na celu sparaliżowanie działania albo spowodowanie zakłóceń w funkcjonowaniu systemu komputerowego lub telekomunikacyjnego[749]. Przestępstwo sabotażu komputerowego zostało stypizowane w art. 269 k.k. Artykuł 269 § 1 k.k. określa typ kwalifikowany – w stosunku do art. 268 § 1 – przestępstwa niszczenia, uszkadzania, usuwania lub wprowadzania bezprawnych zmian danych informatycznych. Przesłanką zaostrzonej karalności jest szczególne znaczenie usuniętych, zniszczonych lub zmienionych informacji dla obronności państwa, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, samorządowej lub innego organu państwowego. Mogą to być np. informacje dotyczące rozmieszczenia broni, systemów dowodzenia, zapisy istotne dla kierowania i kontroli komunikacji kolejowej, drogowej, wodnej lub powietrznej, informacje o podstawowym znaczeniu dla działalności organu państwowego. Karalność obejmuje także zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przesyłania określonych w tym przepisie danych informatycznych.

Tymczasem art. 4 decyzji ramowej 2005/222/WE nakazuje penalizowanie nielegalnej ingerencji w dane, przez co rozumie się podejmowanie wszelkich działań polegających na „bezprawnym usunięciu, uszkodzeniu, pogorszeniu, zmianie, zatajeniu lub uczynieniu niedostępnymi danych komputerowych". Dlatego zakres art. 269 § 1 k.k. należy uznać za zbyt wąski i w obecnym brzmieniu niezgodny z art. 4 decyzji ramowej.

Z kolei przedmiotem ochrony art. 269a k.k. jest niezakłócone funkcjonowanie systemu komputerowego lub sieci teleinformatycznej. Zabronione zachowanie polega na nieuprawnionej transmisji, zniszczeniu, usunięciu, uszkodzeniu lub zmianie danych informatycznych, jeżeli spowodowało to zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej w istotny sposób. Jest to więc przestępstwo materialne, w którym skutek został określony – zdaniem A. Marka[750] – wybitnie celnie. Podmiotem omawianego przestępstwa może być tylko osoba nieuprawniona do ingerencji w pracę określonego systemu komputerowego lub sieci teleinformatycznej. Jest to przestępstwo umyślne, przy czym czynności sprawcze wymagają zamiaru bezpośredniego, natomiast

samo zakłócenie i jego istotność (skutek) może być objęte zamiarem ewentualnym.

Przestępstwo tzw. sabotażu komputerowego zostało określone w art. 3 decyzji ramowej 2005/222/WE w sposób analogiczny do art. 269 i 269a k.k., ponieważ za czyn zabroniony uznano tzw. nielegalną ingerencję w system, czyli poważne naruszenie lub przerwanie funkcjonowania systemu informatycznego (analogiczne rozwiązania przyjęte zostały także w art. 5 konwencji o cyberprzestępczości).

Przepis odnoszący się do bezprawnego wykorzystywania programu komputerowego to art. 269b k.k., który za przestępstwo uznaje wytwarzanie, pozyskiwanie, zbywanie lub też udostępnianie innym osobom urządzeń lub programów komputerowych przystosowanych do popełnienia określonych przez ustawodawcę przestępstw, a także haseł komputerowych, kodów dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej. Oprogramowanie służące do popełnienia przestępstw przeciwko ochronie informacji często określane jest mianem „narzędzi hakerskich" i obejmuje szeroką grupę instrumentów umożliwiających naruszenie integralności danych, sparaliżowanie pracy systemu komputerowego. Można tu wymienić m.in. urządzenia podsłuchowe i wirusy komputerowe.

Artykuł 269b k.k. penalizuje również wytwarzanie, pozyskiwanie, zbywanie oraz udostępnianie innym osobom:

- urządzeń i programów komputerowych przystosowanych do popełnienia przestępstw wymienionych w tym przepisie (choćby jednego);
- haseł i kodów dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej.

Zakres przepisu art. 269b k.k. został przez polskiego ustawodawcę znacznie rozszerzony w stosunku do wzorcowej regulacji z art. 6 konwencji o cyberprzestępczości. Jak podkreśla A. Adamski[751], w odróżnieniu od art. 6 konwencji o cyberprzestępczości art. 269b k.k. nie wymaga od sprawcy działania w zamiarze bezpośrednim, lecz „zadowala się" zamiarem ewentualnym. W rezultacie przepis ten

pozwala na ściganie m.in. operatorów witryn internetowych udostępniających narzędzia programistyczne służące np. do powodowania przeciążeń systemów komputerowych. Z kolei K. Gienas[752] podkreśla, że przepis z art. 269b k.k. stanowi przejaw nadmiernej kryminalizacji życia społecznego. Zauważa on, że w razie nieopatrznej wykładni art. 269b k.k. pod znakiem zapytania stanęłoby przykładowo dalsze funkcjonowanie forów i list dyskusyjnych poświęconych wymianie informacji o szeroko pojętym bezpieczeństwie informatycznym. Z tego względu postuluje on uzupełnienie tego przepisu o klauzulę niekaralności osób wykorzystujących narzędzia hakerskie w celu uprawnionego testowania zabezpieczeń systemów i sieci komputerowych. Sugestia ta wydaje się bardzo trafna i uzasadniona.

Wprowadzenie do polskiego porządku prawnego art. 269b k.k. obejmującego kryminalizację szerokiego spektrum zachowań odnoszących się do instrumentów służących cyberprzestępcom powinno pozytywnie wpłynąć na redukcję liczby zamachów przeciwko ochronie elektronicznie przetwarzanej informacji. W odróżnieniu od klasycznych naruszeń porządku prawnego zamachy skierowane przeciwko szeroko pojętym systemom komputerowym i przetwarzanym za ich pomocą informacjom wymagają bowiem pogłębionej wiedzy i umiejętności lub dostępu do specyficznego instrumentarium informatycznego. Wielu cybernetycznych przestępców nie jest w stanie samodzielnie tworzyć wyrafinowanych narzędzi informatycznych, lecz opierają się na przygotowanych już schematach, często łatwo dostępnych w sieci. Przepis art. 269 k.k. ma utrudniać rozpowszechnianie takich schematów.

Przepis art. 190a został dodany przez art. 1 pkt 2 ustawy z 25 lutego 2011 r. o zmianie ustawy – Kodeks karny[753], która weszła w życie 6 czerwca 2011 r.[754] Głównym przedmiotem ochrony jest tu szeroko rozumiana wolność zarówno w aspekcie wolności „od czegoś" (strachu, nagabywania, niechcianego towarzystwa innej osoby), jak i wolności „do czegoś" (przede wszystkim do zachowania swojej prywatności). Ubocznym przedmiotem ochrony wydają się tu zdrowie człowieka (psychiczne, fizyczne), jego nietykalność cielesna, nienaruszalność korespondencji itp.

W przepisie § 1 ustawodawca posługuje się określeniem „uporczywe nękanie". Trudność zawiera się w interpretacji nękania, którego kodeks nie definiuje. Nie wchodząc bliżej w to złożone zagadnienie, warto jedynie przypomnieć słownikowe znaczenie tego określenia: „ustawicznie dręczyć, trapić, niepokoić kogoś czymś, dokuczać komuś, nie dawać chwili spokoju"[755]. Wydaje się, że znamię nękania realizują jedynie te zachowania, które powodują przykrość pokrzywdzonego, wyrządzają mu krzywdę czy powodują dyskomfort. W pojęciu nękania mieści się niewątpliwie powtarzalność zachowań sprawcy. Problem zaczyna się w momencie, gdy np. pojawia się zdecydowanie za dużo listów czy SMS-ów (np. po kilkanaście czy kilkadziesiąt dziennie), a ich adresat sobie tego nie życzy. Może być również i tak, że już nawet jednostkowe zachowania sprawcy będą stanowiły naruszenie określonych przepisów prawa karnego czy prawa wykroczeń (np. naruszanie miru domowego – art. 193 k.k., groźby – art. 190 § 1 k.k., kradzieże rzeczy należących do pokrzywdzonego – art. 278 k.k., art. 119 k.w., utrwalanie wizerunku nagiej osoby – art. 191a k.k.[756]

Skoro już ze znaczenia słowa „nękać" wynika, że chodzi o wiele zachowań, co jak wcześniej wspomniano oznacza „bezustannie niepokoić" czy „ustawicznie dręczyć" (czyli czynić to wielokrotnie), czy potrzebne jest tworzenie wymagania, aby było to niepokojenie „uporczywie wielokrotne"?[757]

Przestępstwo nękania określone w § 1 ma charakter materialny, konieczne jest wystąpienie skutku w postaci wzbudzenia u pokrzywdzonego uzasadnionego okolicznościami poczucia zagrożenia lub istotnego naruszenia jego prywatności. Szerokie ujęcie skutku można uznać za zasadne, w praktyce bowiem mogą zdarzyć się przypadki zarówno takie, gdy ofiara nękania zaczyna odczuwać lęk, zmienia swoje relacje z innymi osobami czy nawet szuka pomocy u lekarza, jak i takie, gdy nie występuje u niej poczucie zagrożenia. Nawet jeśli poczucia zagrożenia nie ma, ale pokrzywdzony zmuszony jest do istotnych (niekomfortowych) zmian w swoim życiu prywatnym, to zachowanie sprawcy powinno być kryminalizowane. Może dojść do sytuacji, gdy zachowanie sprawcy nie wzbudza poczucia zagrożenia ani też nie narusza istotnie prywatności pokrzywdzonego, jest jednak odbierane przez niego jako uciążliwe (chociaż nie pociąga

za sobą zmiany trybu życia czy przyzwyczajeń pokrzywdzonego). W takim przypadku w grę może wejść konstrukcja usiłowania przestępstwa z art. 190a § 1 k.k.[758] Jest to przestępstwo powszechne i umyślne. Ze względu na występujące w przepisie znamię uporczywości, które jest zabarwione podmiotowo, należy uznać, że ta część znamion musi być objęta zamiarem bezpośrednim. Natomiast należy sądzić, że nie ma przeszkód, aby znamię skutku (w postaci wzbudzenia u pokrzywdzonego poczucia zagrożenia lub istotnego naruszenia jego prywatności) mogło być objęte zamiarem zarówno bezpośrednim, jak i ewentualnym[759].

W przepisie 190a § 2 k.k. kryminalizowane jest podszywanie się pod inną osobę, wykorzystywanie jej wizerunku lub innych jej danych osobowych w celu wyrządzenia jej szkody majątkowej lub osobistej. Jak podkreślano w uzasadnieniu, penalizowane będzie w ten sposób zjawisko przywłaszczenia tożsamości pokrzywdzonego, którego kryminalizacja powinna mieć miejsce na przedpolu skutku. Z uwagi na fakt, że ustawodawca posłużył się słowami „osoba" i „dane osobowe", należy przyjąć, że w grę wchodzi jedynie tożsamość osoby fizycznej[760]. Nie dotyczy ona zatem danych identyfikujących osoby prawnej bądź jednostki organizacyjnej niemającej osobowości prawnej. W doktrynie zauważa się jednak, że informacja o osobie fizycznej może wynikać z informacji o podmiocie zbiorowym, a niekiedy granice między informacjami o osobie fizycznej i podmiocie zbiorowym ulegają zatarciu[761]. Należy uznać, że sprawca musi się podszywać pod inną, rzeczywiście istniejącą osobę, a nie fikcyjną. Przesądza o tym fakt, że dane dotyczące osoby nieistniejącej w realnym świecie nie są danymi osobowymi w świetle ustawy z 10 maja 2018 r. o ochronie danych osobowych[762].

Według A. Zolla znamiona podszywania się realizuje zachowanie polegające na podjęciu przez sprawcę działań jako inna osoba, przy czym zachowanie takie musi być podjęte bez wiedzy i zgody osoby, za którą sprawca się podaje[763]. Jeśli zaś chodzi o określenie „wizerunek", to *Słownik języka polskiego* podaje dwa jego znaczenia: „czyjaś podobizna na rysunku, obrazie, zdjęciu itp." oraz „sposób, w jaki dana osoba lub rzecz jest postrzegana i przedstawiana". Należy sądzić, że na gruncie art. 190a k.k. w grę będą wchodzić oba znaczenia słowa

„wizerunek”. Trzeba zwrócić uwagę, że ustawodawca użył określenia „wizerunek lub inne jej dane osobowe”, a nie sformułowania „wizerunek lub dane osobowe”, tym samym przesądzając, że wizerunek niejako wchodzi w skład danych osobowych.

Przestępstwo stypizowane w art. 190a § 2 k.k. ma charakter powszechny, formalny i może być popełnione jedynie w zamiarze kierunkowym (*dolus directus coloratus*). Budzi jednak wątpliwość, czy zasadne jest zawężenie sfery kryminalizacji jedynie do zachowań z zamiarem kierunkowym („w celu wyrządzenia jej szkody”). Dlaczego ma być wolna od odpowiedzialności osoba, która wykorzystuje wizerunek innej osoby lub jej dane, godząc się jedynie na to, że swoim zachowaniem wyrządzi jej szkodę (majątkową lub osobistą). Nie trzeba również wykazywać, jak trudne jest udowodnienie w procesie karnym strony podmiotowej (a w szczególności istnienia *dolus coloratus*). *De lege ferenda* należy zatem postulować zmianę tego przepisu przez użycie zamiast wyrażenia „w celu” sformułowania „w zamiarze”.[764]

W przepisie § 3 określony został typ kwalifikowany. Jest to konstrukcja podobna jak w przypadku przestępstwa znęcania się (art. 207 § 3). Niewątpliwie może zdarzyć się tak, że „zaszczuta” ofiara przestępstwa nękania, niemogąca już sobie poradzić z występującym problemem, targnie się na swoje życie. Przestępstwo z § 3 ma charakter powszechny, skutkowy (skutkiem jest tu targnięcie się pokrzywdzonego na swoje życie), może być ono popełnione z winy kombinowanej (*culpa dolo exorta* – art. 9 § 3).

Przestępstwa z art. 190a § 1 oraz art. 190a § 2 są ścigane na wniosek pokrzywdzonego, typ kwalifikowany (§ 3) zaś – z urzędu. Takie zróżnicowanie należy uznać za zasadne, ponieważ dobro zagrożone w typie kwalifikowanym ma zdecydowanie większą wartość niż w przypadku dóbr chronionych przepisami § 1 i 2. Jest to również wyraz konsekwencji ustawodawcy, inne bowiem typy przestępstw, w których przypadku dochodzi do targnięcia się pokrzywdzonego na swoje życie, również są ścigane z urzędu (art. 207 § 3, art. 352 § 3).

Przepisy art. 190a § 1 mogą pozostawać w rzeczywistym właściwym zbiegu z innymi przepisami. Rzeczywisty niewłaściwy zbieg zachodzi między przepisami art. 190a § 1 a przepisem art. 191 § 1 (zmuszanie),

art. 193 (naruszenie miru domowego), art. 212 (zniesławienie), art. 216 (zniewaga), art. 217 § 1 (naruszenie nietykalności cielesnej), które to przypadki rozwiązywane są przy zastosowaniu zasady *lex consumens derogat legi consumptae* (gdzie przepisem pochłaniającym jest art. 190a).

Zdaniem A. Lacha w przypadku zbiegu przepisów art. 190a i 212 k.k. „czyn należy kwalifikować z art. 190a § 2 k.k. jako *lex specialis*”[765]. Największy problem stanowi wzajemna relacja zachodząca między przepisami art. 190a a art. 207 k.k., gdzie w zależności od konkretnego stanu faktycznego możliwy jest zarówno zbieg pomijalny, jak i kumulatywna kwalifikacja. W przypadku przepisu art. 190a § 2 k.k. może on pozostawać w rzeczywistym niewłaściwym zbiegu z przepisami typizującymi przestępstwa przeciwko ochronie informacji (art. 265–268a, 269a k.k.), przeciwko wiarygodności dokumentów (art. art. 270, 272, 273 i 275 k.k.). Niewątpliwie w praktyce może również pojawić się kumulatywna kwalifikacja przepisu art. 190a § 2 k.k. z art. 49 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (kryminalizującym niedopuszczalne przetwarzanie danych osobowych), jak również z art. 115 ust. 1 ustawy z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[766].

Oszustwo komputerowe jako nowy typ przestępstwa wprowadzono w celu wypełnienia luki, jaka powstała w tradycyjnym pojęciu oszustwa w wyniku postępu technicznego i szybkiego rozwoju komunikacji elektronicznej. Okazało się, że w naszych czasach klasyczna postać oszustwa stała się nieadekwatna, gdyż na skutek automatyzacji wielu procesów wymiany dóbr i usług, relacje interpersonalne zastąpiły relacje człowiek – maszyna.

Przestępstwo tzw. oszustwa komputerowego, podobnie jak przestępstwo fałszerstwa komputerowego, zostało stypizowane w *Konwencji Rady Europy o cyberprzestępczości* (art. 8)[767], natomiast decyzja ramowa nie odnosi się do tego przestępstwa. Czyn objęto także przepisami polskiego *Kodeksu karnego*.

W prawie polskim przestępstwa oszustwa komputerowego może dopuścić się każdy, kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych

informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych (art. 287 k.k.)[768]. Przykładem typowego oszustwa komputerowego może być włamanie się do sieci komputerowej w banku i wydanie dyspozycji wykonania przelewu określonej kwoty na rachunek sprawcy, pomnożenia kwoty już na rachunku sprawcy, zmniejszenia jego pasywów czy przelanie pieniędzy osoby trzeciej na rachunek fundacji dobroczynnej.

W praktyce oszustwa komputerowe przyjmują postać:

- manipulowania danymi wprowadzanymi do systemu (na wejściu);
- manipulowania programem komputerowym;
- manipulowania rezultatami przetwarzanych danych (na wyjściu)[769].

W pierwszym przypadku działanie sprawcy ogranicza się do wprowadzenia do systemu nieprawdziwych danych w celu uzyskania korzyści majątkowej (np. zlecenie przez pracownika banku dokonania elektronicznego przelewu na własny rachunek bankowy). W drugim przypadku sprawca manipuluje istniejącym programem komputerowym w taki sposób, aby wykonywał on dodatkowe operacje umożliwiające dokonywanie nadużyć (najczęstszym przykładem jest modyfikacja programu obliczającego salda na rachunkach bankowych w ten sposób, aby zaokrąglał salda zawsze „w dół", przelewając jednocześnie nadwyżki na ustalony rachunek bankowy sprawcy). W trzecim przypadku sprawca manipuluje rezultatami przetwarzania danych, co pozwala mu na osiąganie korzyści majątkowych.

Polski ustawodawca zdecydował się na przyjęcie innego niż przedstawiony wcześniej podziału oszustw komputerowych. W przepisie art. 287 k.k. mamy do czynienia z dwoma grupami czynności sprawczych, do których należą:

- wpływanie na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji;
- zmienianie, usuwanie lub wprowadzanie nowego zapisu danych informatycznych.

Do pierwszej grupy czynności sprawczych zaliczamy zarówno manipulacje danymi wprowadzanymi do systemu, jak i manipulacje

rezultatami przetwarzanych danych, a więc zmiany dokonywane na wejściu do komputera lub też na jego wyjściu. Wpływaniem będzie także mechaniczna ingerencja w urządzenie, np. uszkodzenie lub połączenie z innym urządzeniem. Do drugiej grupy czynności sprawczych należą czynności polegające na zmianie zapisu kodowego zamieszczonego na nośniku informacji. Zmiana może być dokonywana bezpośrednio na komputerze lub przez włamanie się do sieci łączącej komputer z podobnymi urządzeniami[770].

Ze względu na umieszczenie przestępstwa z art. 287 k.k. w rozdziale, w którym mowa jest o przestępstwach przeciwko mieniu, można stwierdzić, że zasadniczym przedmiotem ochrony jest w tym przypadku mienie, przy czym z uwagi na kształt znamion tego przestępstwa oraz ustawowy kontekst pojęcie to należy rozumieć jako zbiorczą nazwę wszelkich praw majątkowych, których potwierdzeniem (dowodem istnienia) jest odpowiedni zapis w systemie gromadzącym, przetwarzającym lub przesyłającym automatycznie dane informatyczne albo mienie, z którym taki zapis jest związany. Przestępstwo to chroni więc przed wszelkimi działaniami oszukańczymi własność lub inne prawa rzeczowe albo obligacyjne do mienia, wyrażone w postaci zapisu na odpowiednim nośniku informacji. Ponadto jako dobro poboczne chronione są zapisy informacji oraz zasady automatycznego ich przetwarzania, gromadzenia lub przesyłania.

Biorąc pod uwagę kryterium określenia strony podmiotowej tego przestępstwa, czyny ujęte w art. 287 k.k. można również podzielić na tzw. oszustwo komputerowe[771] oraz szkodnictwo komputerowe[772]. W literaturze[773] można spotkać pogląd, że zamierzeniem twórców artykułu penalizującego oszustwo komputerowe nie było wyodrębnianie przestępstwa o charakterze materialnym. Skutkowe ujęcie przestępstwa zwanego oszustwem komputerowym mogłoby bowiem prowadzić do pozostawienia poza nawiasem odpowiedzialności karnej wielu zachowań godzących bezpośrednio w urządzenia i systemy komputerowe. Zachowanie sprawcy determinowane chęcią osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, nieprowadzące do przekształceń i zmian w świecie zewnętrznym, pozostałoby tym samym poza

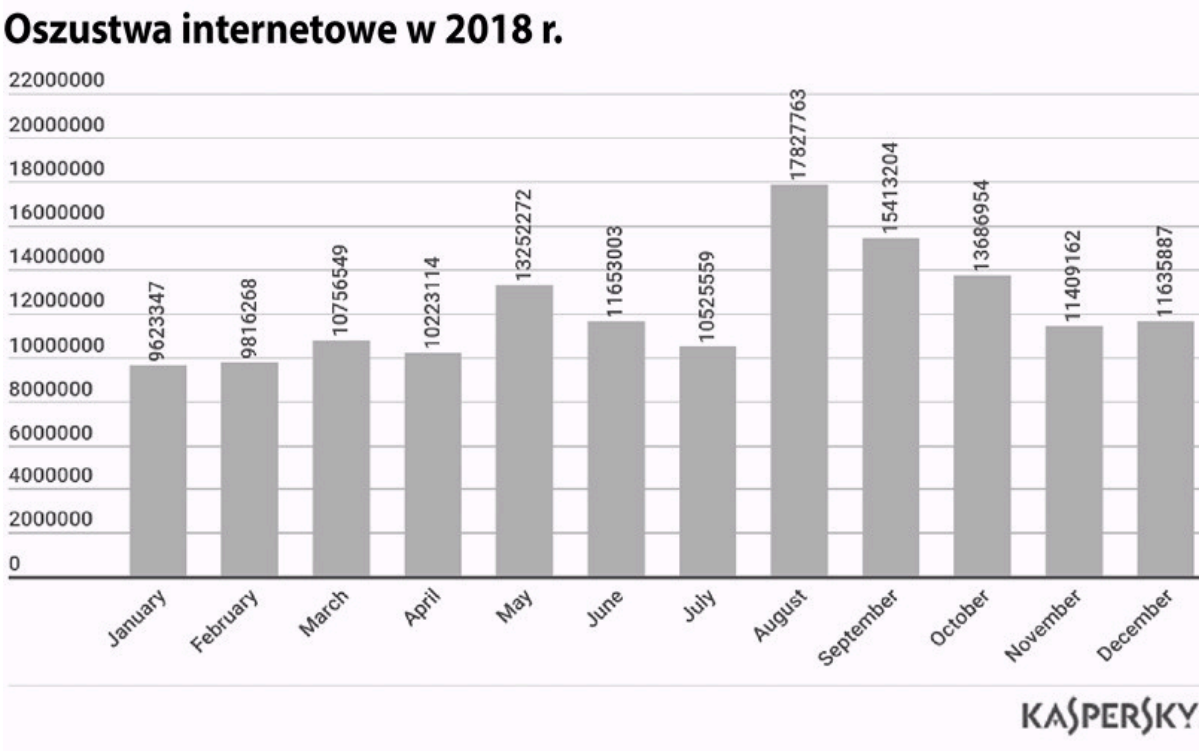
zakresem penalizacji art. 287 k.k. Takiego niebezpieczeństwa nie stwarza natomiast formalne ujęcie oszustwa komputerowego, wymieniony sposób działania sprawcy zostanie bowiem objęty karalnymi znamionami wpływania na automatyczne przetwarzanie informacji[774]. W wielu publikacjach można znaleźć także głosy przeciwne[775], uznające przestępstwo z art. 287 k.k. za przestępstwo skutkowe (materialne), do którego znamion należy skutek w postaci dokonania zmiany (wpływu) w automatycznym przetwarzaniu, gromadzeniu lub przesyłaniu informacji lub dokonanie zmiany, usunięcie albo wprowadzenie nowego zapisu na komputerowym nośniku informacji.

Przyjmuje się, że art. 287 § 1 k.k. to *lex specialis* do art. 268, 268a oraz 269a k.k. Często można także spotkać się z kumulacją art. 287 i 267 lub 279 k.k. W szczególnych przypadkach, gdy dane informatyczne, o których mowa w art. 287 k.k., będą jednocześnie zawierały informacje o szczególnym znaczeniu dla obronności państwa, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, funkcjonowania innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego, będzie można mówić o kumulatywnym zbiegu art. 287 z art. 269 § 2 k.k.

Jeśli chodzi o oszustwa komputerowe, warto zaznaczyć, że w *Kodeksie karnym* uregulowano także tzw. oszustwo telekomunikacyjne (art. 285 § 1)[776]. Włączenie się do urządzenia telekomunikacyjnego może przybrać postać fizycznej ingerencji w integralność urządzenia, np. przez przecięcie przewodów i podłączenie się do linii telefonicznej, bądź ingerencji logicznej, czyli ingerencji w oprogramowanie stanowiące integralną część urządzenia. W szczególności ta druga z postaci związana jest z działalnością *phreakerów*[777].

Podsumowując rozważania, należy stwierdzić, że art. 287 k.k. daje podstawę inkryminowania oszustwa zarówno komputerowego, jak i telekomunikacyjnego, gdyż w niektórych przypadkach ciężko wyznaczyć granicę między tymi dwoma przestępstwami. Warto też zwrócić uwagę na regulację z art. 295 k.k. W przypadku uznania oszustwa komputerowego za przestępstwo formalne, przepis ten wadliwie premiuje czyny, których skutkiem jest szkoda, pozwalając na

stosowanie nadzwyczajnego złagodzenia kary, w sytuacji gdy sprawca dobrowolnie naprawi wyrządzoną szkodę. Z uwagi na to, że przepis z art. 295 k.k. może mieć zastosowanie dopiero wtedy, gdy powstanie szkoda, nie można go stosować w przypadku, gdy do ujawnienia przestępstwa komputerowego dojdzie w początkowej jego fazie. W związku z tym regulację tę należy ocenić krytyczne, gdyż wadliwie pozwala ona na zastosowanie złagodzenia kary w przypadku zachowań o wyższej szkodliwości społecznej, a wyklucza w przypadku zachowań mniej szkodliwych, dopiero zmierzających do wyrządzenia szkody. Należy zaznaczyć, że obecnie naprawienie szkody w przypadku przestępstw, których skutkiem będzie elektroniczne przesłanie środków pieniężnych na konto sprawcy, może być bardzo proste i trwać kilka sekund. Paradoksalnie więc przyznanie sprawcy oszustw komputerowych możliwości ubiegania się o nadzwyczajne złagodzenie kary lub odstąpienie od jej wymierzenia pod warunkiem dobrowolnego naprawienia szkody może zachęcać do popełniania takich przestępstw, co z pewnością nie było intencją ustawodawcy[778].



RYSUNEK 6.5 Oszustwa internetowe w Polsce w 2018 r.

Źródło: Raport Kaspersky za 2018 r.

6.2.3. WYMIAR INSTYTUCJONALNY ZWALCZANIA CYBERTERRORYZMU W POLSCE

System ochrony cyberprzestrzeni w Polsce ma charakter zdecentralizowany, a kompetencje dotyczące cyberbezpieczeństwa mogą być realizowane przez Ministra Obrony Narodowej, szefa Agencji Bezpieczeństwa Wewnętrznego, Ministra Spraw Wewnętrznych i Administracji, policję, Rządowe Centrum Bezpieczeństwa czy też Ministra Cyfryzacji. Cyberbezpieczeństwem zajmują się także zespoły CSIRT utworzone przez operatorów telekomunikacyjnych, banki, przedsiębiorstwa energetyczne oraz środowiska naukowo-badawcze. Wymienione podmioty realizują zadania w zakresie cyberbezpieczeństwa w sferze cywilnej, zwalczania cyberprzestępczości, zapobiegania zdarzeniom terrorystycznym i obrony narodowej.

Zgodnie z art. 146 ust. 4 pkt 7 i 11 Konstytucji RP[779] Rada Ministrów zapewnia bezpieczeństwo wewnętrzne państwa i porządek publiczny oraz sprawuje ogólne kierownictwo w dziedzinie obronności kraju. Ustawa z dnia 4 września 1997 r. o działach administracji rządowej[780] definiuje działy administracji rządowej (w tym dział sprawy wewnętrzne obejmujący kwestie bezpieczeństwa wewnętrznego i porządku publicznego oraz dział obrona narodowa), które są następnie przypisywane poszczególnym ministrom.

Za kreowanie polityki bezpieczeństwa teleinformatycznego związanej z funkcjonowaniem systemów i sieci teleinformatycznych resortu odpowiada pełnomocnik ministra obrony narodowej ds. bezpieczeństwa cyberprzestrzeni. Minister Cyfryzacji zgodnie z ustawą o usługach zaufania i identyfikacji elektronicznej zapewnia również funkcjonowanie krajowej infrastruktury zaufania oraz sprawuje nadzór nad dostawcami usług zaufania.

Zgodnie z art. 7 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[781] Rada Ministrów sprawuje zarządzanie kryzysowe na terytorium RP (w przypadkach niecierpiących zwłoki minister właściwy ds. wewnętrznych). Rządowy Zespół Zarządzania Kryzysowego jest organem opiniodawczo-doradczym przy Radzie Ministrów. Do jego zadań należy:

- przygotowywanie propozycji użycia sił i środków niezbędnych do opanowania sytuacji kryzysowych;
- doradzanie w zakresie koordynacji działań organów administracji rządowej, instytucji państwowych i służb w sytuacjach kryzysowych;
- opiniowanie sprawozdań końcowych z działań podejmowanych w związku z zarządzaniem kryzysowym;
- opiniowanie potrzeb dotyczących odtwarzania infrastruktury lub przywrócenia jej pierwotnego charakteru;
- opiniowanie i przedkładanie Radzie Ministrów *Krajowego Planu Zarządzania Kryzysowego*;
- opiniowanie projektu zarządzenia Prezesa Rady Ministrów w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego[782].

Organizatorem systemów i sieci teleinformatycznych jest szef Inspektoratu Systemów Informacyjnych. Ważną rolę w obszarze bezpieczeństwa cyberprzestrzeni pełni także Narodowe Centrum Kryptologii, które jako organ Sił Zbrojnych RP zajmuje się wdrażaniem rozwiązań kryptograficznych na potrzeby polskiej administracji publicznej i wojska. Do głównych zadań NCK należy realizacja zadań związanych z prowadzeniem badań, projektowaniem, budową, wdrażaniem, użytkowaniem oraz ochroną narodowych technologii kryptologicznych, a także wytwarzanie nowych produktów dla państwa przez zespolenie potencjału naukowego i przemysłowego w obszarze zaawansowanych technologii informatycznych i kryptograficznych[783].

W Polsce wiodącą rolę w działaniach antyterrorystycznych odgrywają dwie instytucje: Agencja Bezpieczeństwa Wewnętrznego (ABW)[784] i policja[785]. Chociaż podział ich obowiązków nie jest jasny, te dwie instytucje ściśle ze sobą współpracują, ponieważ terroryzm stanowi poważne zagrożenie dla dobra publicznego każdego państwa. Agencja Bezpieczeństwa Wewnętrznego jest służbą specjalną odpowiedzialną za kwestie związane z ochroną bezpieczeństwa wewnętrznego państwa i jego konstytucyjnego porządku. Głównym zadaniem ABW jest zwalczanie różnego rodzaju zagrożeń dla

bezpieczeństwa wewnętrznego państwa, jak przestępstwo szpiegostwa, terroryzmu, handlu narkotykami na skalę międzynarodową. Działania pozwalające zapobiegać rozwojowi przestępczości zorganizowanej wynikają z uprawnień operacyjno-rozpoznawczych oraz dochodzeniowo-śledczych, które pomagają wykryć przestępstwo, a także ścigać jego sprawców. Czynności operacyjno-rozpoznawcze i analityczno-informacyjne służą głównie pozyskaniu informacji dla zapewnienia bezpieczeństwa państwa i wspomnianego wcześniej ładu zagwarantowanego Konstytucją RP. Istotne jest jednak, że ABW w sprawnym zwalczaniu przestępczości zorganizowanej nie posługuje się żadnymi instrumentami o prawnym podłożu. Wynika to z braku konkretnych uregulowań ustawowych, które miałyby zagwarantować taki status.

Zgodnie z ustawą z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[786] i ustawą z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych ABW odpowiada za rozpoznawanie, zapobieganie i wykrywanie zagrożeń sieci teleinformatycznych istotnych dla państwa, przeprowadzanie oceny bezpieczeństwa systemów, wskazywanie podatności, żądanie „blokady dostępności", prowadzenie rejestru zdarzeń naruszających bezpieczeństwo, analizę naruszeń i wydawanie rekomendacji. Policja wykonuje zadania z zakresu zwalczania cyberprzestępczości (w strukturze Komendy Głównej Policji funkcjonuje Biuro do Walki z Cyberprzestępczością).

Warto zaznaczyć, że z dniem 1 lutego 2008 r. został powołany Rządowy Zespół Reagowania na Incydenty Komputerowe (CERT.GOV.PL). Jest to jednostka działająca w strukturach Agencji Bezpieczeństwa Wewnętrznego, będąca częścią Departamentu Bezpieczeństwa Teleinformatycznego[787]. Jej główną misją jest nauka i szkolenie instytucji państwowych funkcjonujących w Polsce skutecznej ochrony przed atakami z sieci. Do jej zadań należy również:

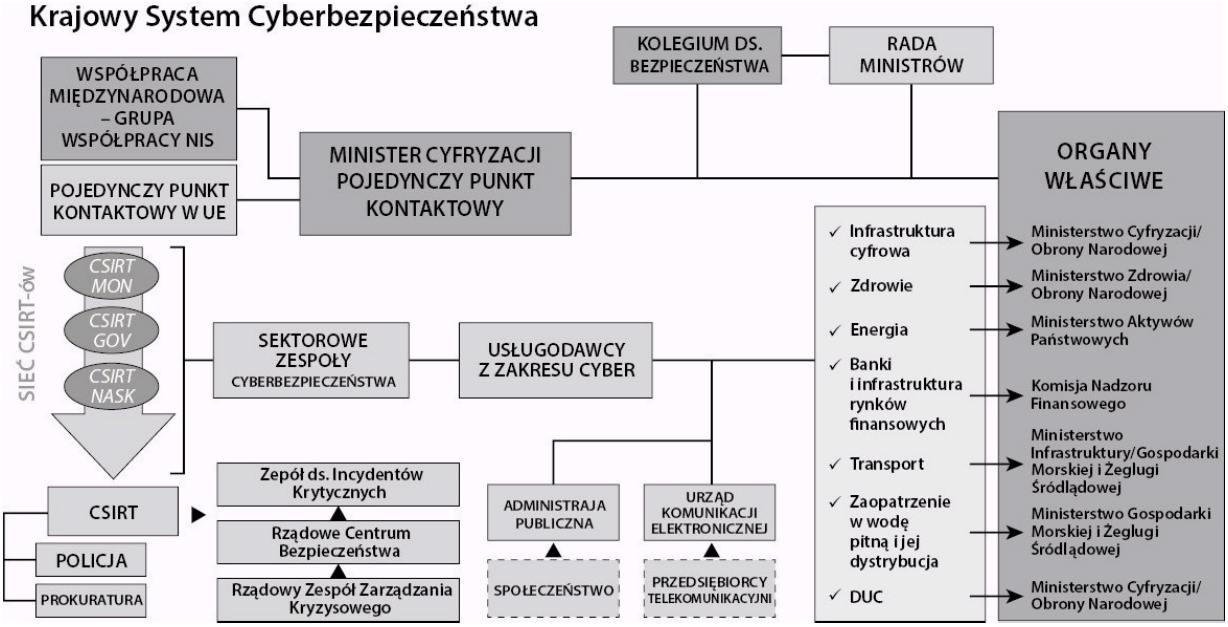
- koordynowanie odpowiadania na zdarzenia dotyczące ataków w Internecie;
- wydawanie i ogłaszanie alarmów;

- zajmowanie się przyjętymi zgłoszeniami, w tym kompletowanie dowodów przez specjalnie powołany do tego zespół biegłych sądowych;
- zajmowanie się incydentami w systemach, które znajdują się pod ochroną ARAKIS-GOV;
- wykonywanie badań dotyczących bezpieczeństwa w sieci[788].

Działalność zespołu zaowocowała stworzeniem systemu ARAKIS-GOV jako narzędzia służącego do wczesnego ostrzegania o zagrożeniach w sieci Internet oraz wdrożeniem *Programu badania bezpieczeństwa witryn internetowych administracji publicznej*, stosowanego do określanie poziomu bezpieczeństwa aplikacji „www" instytucji publicznych oraz usuwania wykrytych nieprawidłowości, zanim zostaną wykorzystane przez cyberprzestępców[789].

CERT na bieżąco zbiera i analizuje informacje o atakach i zagrożeniach. Jednym z jego zadań jest nadzór nad systemem wczesnego ostrzegania o incydentach sieciowych ARAKIS-GOV. Prowadzi rutynową akcję monitorowania bezpieczeństwa rządowych witryn internetowych.

W Polsce funkcjonują różne zespoły CSIRT, jednak tylko trzy działają od lat w ramach swojej właściwości na poziomie krajowym. Zamiast tworzyć nowe podmioty, projekt ustawy nadają określone zadania istniejącym podmiotom, które w ramach swojej działalności zajmują się reagowaniem na incydenty komputerowe.



RYSUNEK 6.6
Krajowy system cyberbezpieczeństwa w Polsce
Źródło: cert.gov.pl (dostęp: 03.06.2020).

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL pełni funkcję głównego Zespołu CERT odpowiadającego za koordynację procesu reagowania na incydenty komputerowe występujące w obszarze administracji rządowej oraz infrastruktury krytycznej. Do jego zadań należy rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym.

System Reagowania na Incydenty Komputerowe Resortu Obrony Narodowej (SRnIK RON**)** realizuje zadania w zakresie koordynacji procesów zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach i sieciach teleinformatycznych resortu

obrony narodowej. Zgodnie z założeniami NATO w skład struktury organizacyjnej SRnIK RON wchodzą Centrum Koordynacyjne SRnIK, Centrum Wsparcia SRnIK, które realizuje zadania zgodne z zakresem działania zespołów CERT, oraz administratorzy systemów teleinformatycznych jednostek i komórek organizacyjnych RON. Do głównych zadań SRnIK należy koordynacja reagowania na incydenty komputerowe, obsługa i analiza zdarzeń oraz incydentów, a także prowadzenie działań zmierzających do wzrostu świadomości dotyczącej bezpieczeństwa teleinformatycznego. W ramach podejmowanych zadań SRnIK współpracuje z jednostkami i komórkami organizacyjnymi resortu obrony narodowej oraz z organizacjami pozaresortowymi, krajowymi i międzynarodowymi.

W lipcu 2016 r. w ramach NASK zostało powołane Narodowe Centrum Cyberbezpieczeństwa[790] (NC Cyber). Jest to centrum szybkiego reagowania na zagrożenia i zgłaszane incydenty w cyberprzestrzeni, a w razie ewentualnych ataków – podejmowania koniecznych działań we współpracy z ośrodkami w kraju i za granicą w zakresie przeanalizowania natury, sposobu, zasięgu incydentu oraz wymiany informacji w celu ostrzeżenia kluczowych sektorów i instytucji. NC Cyber wydaje rekomendację postępowania w obliczu zagrożenia oraz koniecznych działań minimalizujących skutki zagrożenia. Centrum operacyjne NC Cyber funkcjonuje w trybie 24/7, 365 dni w roku. Jego działalność opiera się na kilku filarach: operacyjnym, analitycznym, badawczo-rozwojowym, szkoleniowym oraz obszarze polityk i standardów. Celem jego powołania była rozbudowa funkcji operacyjnych i analityczno-technicznych, aby można było zarządzać bezpieczeństwem cyberprzestrzeni w krytycznych dla państwa i gospodarki obszarach działalności oraz budować kompetencje w obszarze strategicznym.

Podmioty publiczne i prywatne mogą współpracować z NC Cyber na podstawie zawartych porozumień w zakresie cyberbezpieczeństwa, a także delegować swoich przedstawicieli do bieżącej współpracy. Porozumienia o współpracy zostały już podpisane z ponad 40 podmiotami, w tym przedstawicielami sektorów telekomunikacyjnego, finansowego (banków i instytucji finansowych), energetycznego, kolejowego, dostawcami usług cyfrowych. Zostały zbudowane kanały

komunikacji między uczestniczącymi podmiotami (strefa partnera, system informowania o incydentach – MISP).

Jako szczególnie ważną i konieczną należy uznać propozycję ustalenia odpowiedzialności za ochronę cyberbezpieczeństwa RP z podaniem zakresów zadań, odpowiedzialności i zmian w strukturach organizacyjnych niektórych organów administracji (w tym Prezesa Rady Ministrów, Ministra Spraw Wewnętrznych, Ministra Obrony Narodowej, Agencji Bezpieczeństwa Wewnętrznego) oraz powołania pełnomocników ds. ochrony cyberprzestrzeni (pełnomocnika rządu, pełnomocników w podmiotach administracji, zalecenie utworzenia takiej roli u przedsiębiorców). Działania te przyczyniłyby się do stworzenia trwałego systemu koordynacji i wymiany informacji między podmiotami odpowiedzialnymi za ochronę cyberprzestrzeni oraz władającymi zasobami stanowiącymi krytyczną infrastrukturę teleinformatyczną państwa.

Centralne Biuro Śledcze Policji (CBŚP)[791], które zajmuje się najpoważniejszymi przestępstwami zorganizowanymi o charakterze transgranicznym, kryminalnym, narkotykowym i ekonomicznym oraz terroryzmem, zastąpiło Centralne Biuro Śledcze KGP, czyli komórkę organizacyjną dotychczas funkcjonującą w strukturze Komendy Głównej Policji na podstawie nowelizacji ustawy o Policji z dnia 26 czerwca 2014 r.[792] Od dnia wejścia w życie ustawy zmieniającej, tj. od 9 października 2014 r., służba śledcza funkcjonuje w strukturze odrębnej jednostki organizacyjnej policji – Centralnego Biura Śledczego Policji. W jego strukturze wyodrębniono Wydział do Zwalczania Cyberprzestępczości, który realizuje następujące zadania:

- operacyjne, mające na celu rozpoznawanie i zwalczanie przestępczości zorganizowanej oraz zagrożeń terrorystycznych i ekstremistycznych w cyberprzestrzeni;
- związane z technicznym wspieraniem czynności operacyjnych prowadzonych przez komórki organizacyjne CBŚP przy wykorzystaniu dostępnych narzędzi informatycznych oraz współdziałaniem w tym zakresie z innymi jednostkami organizacyjnymi policji.

W ramach współpracy z Interpolem i Europolem policja podejmuje wspólne przedsięwzięcia mające na celu odpowiednie przygotowanie kadr policji do zwalczania rosnącej i rozwijającej się cyberprzestępczości[793].

Inne instytucje biorące udział w antyterrorystycznej działalności to:

- Agencja Wywiadu (AW) [794],
- Generalny Inspektor Informacji Finansowej (GIIF)[795],
- Straż Graniczna (SG)[796].

Agencja Wywiadu działa, zapewniając bezpieczeństwo zewnętrzne państwa za pośrednictwem konkretnego katalogu zadań wyliczonych w ustawie o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Do tych zadań zgodnie z art. 6 ust. 1 ustawy należy:

- uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej oraz jej potencjału ekonomicznego i obronnego;
- rozpoznawanie i przeciwdziałanie zagrożeniom zewnętrznym godzącym w bezpieczeństwo, obronność, niepodległość i nienaruszalność terytorium Rzeczypospolitej Polskiej;
- rozpoznawanie międzynarodowego terroryzmu, ekstremizmu oraz międzynarodowych grup przestępczości zorganizowanej;
- rozpoznawanie międzynarodowego obrotu bronią, amunicją i materiałami wybuchowymi, środkami odurzającymi i substancjami psychotropowymi oraz towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także rozpoznawanie międzynarodowego obrotu bronią masowej zagłady i zagrożeń związanych z rozprzestrzenianiem tej broni oraz środków jej przenoszenia.

Główną rolę w systemie zwalczania przestępstw finansowych i finansowania terroryzmu odgrywa Generalny Inspektor Informacji Finansowej (GIIF). Do jego zadań należy:

- przeprowadzanie procedury wstrzymania transakcji lub blokady rachunku;
- udostępnianie i żądanie przekazania informacji o transakcjach;

- przekazywanie uprawnionym organom dokumentów uzasadniających podejrzenie popełnienia przestępstwa;
- sprawowanie kontroli przestrzegania przepisów dotyczących przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu;
- współpraca z zagranicznymi instytucjami i międzynarodowymi organizacjami[797].

W październiku 2009 r. przy Generalnym Inspektorze Informacji Finansowej powołano Międzyresortowy Komitet Bezpieczeństwa Finansowego pełniący funkcję opiniodawczą i doradczą w zakresie stosowania szczególnych środków ograniczających przeciwko osobom, grupom i podmiotom, tj. zamrożenia wartości majątkowych w celu zwalczania terroryzmu i przeciwdziałania jego finansowaniu[798].

Instytucją odpowiedzialną za gromadzenie informacji o podejrzanych transakcjach finansowych jest Polska Jednostka Analityki Finansowej (PJAF) – Departament Informacji Finansowej w Ministerstwie Finansów. PJAF weryfikuje zawarte w raportach podejrzenia „prania pieniędzy" i finansowania terroryzmu, a następnie zbiera materiał dowodowy i zawiadamia prokuraturę, która we współpracy z organami ścigania podejmuje działania w celu postawienia aktu oskarżenia osobom podejrzanym. PJAF jest nadzorowana przez Generalnego Inspektora Informacji Finansowej (GIIF). Na forach międzynarodowych PJAF uczestniczy w pracach m.in. MONEYVAL oraz Grupy Egmont (FIU)[799].

Zgodnie z art. 1 ust. 2 pkt 5d ustawy o Straży Granicznej do zadań tej instytucji należy „współdziałanie z innymi organami i służbami w zakresie rozpoznawania zagrożeń terroryzmem i przeciwdziałania tym zagrożeniom".

Na tej podstawie Straż Graniczna, realizując swoje zadania, może wejść w posiadanie informacji, zidentyfikować zjawiska czy ujawnić zdarzenia mogące mieć związek z zagrożeniami terrorystycznymi. Do zadań Straży Granicznej należy:

- rozpoznawanie, zapobieganie i wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców, w szczególności przestępstw pozostających w związku z przekraczaniem granicy państwowej lub przemieszczaniem przez tę granicę towarów oraz

przedmiotów określonych w przepisach o broni, amunicji i materiałach wybuchowych;
- zapewnienie bezpieczeństwa w międzynarodowej komunikacji lotniczej przez prowadzenie kontroli bezpieczeństwa pasażerów, bagaży, ładunków i statków powietrznych realizujących loty wysokiego ryzyka oraz prowadzenie działań minersko-pirotechnicznych;
- utrzymanie ładu i porządku publicznego w zasięgu terytorialnym przejść granicznych, w tym ochrona obiektów należących lub użytkowanych przez Straż Graniczną przed aktami terrorystycznymi;
- zapobieganie przekroczeniu granicy przez osoby niepożądane w RP oraz zatrzymywanie osób poszukiwanych przez organy ścigania;
- zapewnienie bezpieczeństwa w portach lotniczych i morskich ze względu na ich znaczenie strategiczne;
- gromadzenie i analizowanie informacji dotyczących obywateli państw tzw. podwyższonego ryzyka, przekraczających granicę państwową na przejściach granicznych lub usiłujących przekroczyć ją nielegalnie poza przejściami;
- monitorowanie środowisk i skupisk osób pochodzących z państw tzw. podwyższonego ryzyka, powiązanych z przestępczością graniczną;
- współdziałanie i prowadzenie wymiany oraz weryfikacji informacji w zakresie przeciwdziałania zagrożeniom terrorystycznym z Agencją Bezpieczeństwa Wewnętrznego, Agencją Wywiadu, Służbą Kontrwywiadu Wojskowego, Służbą Wywiadu Wojskowego, policją, Biurem Ochrony Rządu, Ministerstwem Finansów, Ministerstwem Spraw Zagranicznych, Żandarmerią Wojskową oraz z organami ochrony granicy państw sąsiednich, jak również innymi służbami i instytucjami.

Należy także wymienić dwa inne organy, które nie biorą udziału w działaniach operacyjnych – Radę Bezpieczeństwa Narodowego (RBN) oraz Biuro Bezpieczeństwa Narodowego (BBN). RBN jest organem doradczym prezydenta Rzeczypospolitej Polska i jest odpowiedzialna

za określenie generalnego planu i celów w zakresie bezpieczeństwa, stosunków międzynarodowych i sił zbrojnych. Z kolei Biuro Bezpieczeństwa Narodowego jest częścią Kancelarii Prezydenta i w myśl art. 11 ustawy o powszechnym obowiązku obrony RP[800] zapewnia mu wsparcie w zakresie wypełniania zadań dotyczących nienaruszalności granic i niepodległości kraju.

Obecnie w Polsce kwestie zabezpieczania systemów teleinformatycznych są regulowane sektorowo lub wycinkowo, według zadań różnych podmiotów. Istnieją regulacje dotyczące zapewnienia systemu zarządzania bezpieczeństwem informacji w podmiotach publicznych[801], zwalczania cyberprzestępczości, zapobiegania zagrożeniom o charakterze terrorystycznym[802] bądź zarządzania kryzysowego[803]. Istnieją również regulacje dotyczące np. konieczności zabezpieczenia usług świadczonych przez przedsiębiorców telekomunikacyjnych[804] czy banki[805].

Warto dodać, że żadna w wymienionych regulacji nie ujmuje problemu całościowo. Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych jest ograniczona do zasad prowadzenia działań antyterrorystycznych oraz współpracy między organami właściwymi w zakresie prowadzenia tych działań. Przepisy ustawy o zarządzaniu kryzysowym odnoszą się do działań związanych z zapobieganiem i zarządzaniem w sytuacjach kryzysowych. Ustawy regulujące pracę organów ścigania, np. ustawa z dnia 6 kwietnia 1990 r. o Policji[806] czy też ustawa z dnia 6 czerwca 1997 r. – Kodeks karny obejmują kwestie związane z zapobieganiem i zwalczaniem przestępstw w cyberprzestrzeni.

Pewne elementy o charakterze bezsankcyjnym, regulujące wymagania bezpieczeństwa teleinformatycznego, odnoszące się do sfery infrastruktury krytycznej zostały zawarte w załączniku nr 1 do *Narodowego Programu Ochrony Infrastruktury Krytycznej* (NPOIK), przyjmowanego na podstawie ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[807]. Rządowe Centrum Bezpieczeństwa weryfikuje plany operatorów infrastruktury krytycznej m.in. pod kątem oceny ryzyka, stosowanych zabezpieczeń i przyjętych w obiektach zasad ochrony teleinformatycznej. Należy podkreślić, że inna jest podstawa prawna dyrektywy 2016/1148, którą jest art. 114

TRUE odnoszący się do wspólnego rynku. Kwestia ochrony państwowej infrastruktury krytycznej jest natomiast kompetencją wyłączną państw członkowskich, ściśle powiązaną ze sferą bezpieczeństwa narodowego, nieobjętą traktatami unijnymi.

Pewne wymagania w zakresie bezpieczeństwa informacji dotyczące zarówno przedsiębiorców, jak i jednostek sektora finansów publicznych znajdują się w ustawie z dnia 6 czerwca 1997 r. – Kodeks karny[808], ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[809], ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych[810], ustawie z dnia 29 września 1994 r. o rachunkowości[811], ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej[812], ustawie z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej[813], ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia[814], ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach[815], ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe, ustawie z dnia 5 września 2016 r. o usługach zaufania i identyfikacji elektronicznej[816], ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[817], ustawie z dnia 29 czerwca 1995 r. o statystyce publicznej[818] oraz ustawie z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji[819].

6.2.4. DYREKTYWA NIS W PRAWIE POLSKIM

Dyrektywa 2016/1148 (NIS) wprowadza mechanizmy współpracy na dwóch poziomach: technicznym i polityczno-strategicznym[820]. Współpraca techniczna ma być zapewniona przez europejską sieć CISRT oraz stworzenie mechanizmów wymiany informacji o incydentach transgranicznych między CSIRT wyznaczonymi dla operatorów usług kluczowych oraz dostawcami usług cyfrowych. Współpraca na poziomie polityczno-strategicznym ma być realizowana przez utworzenie Grupy Współpracy, która zajmie się wypracowaniem wspólnych koncepcji strategicznych i będzie przyjmowała m.in. roczne raporty od właściwych organów. Najważniejsze jest jednak to, że dyrektywa NIS stanowi harmonizację minimalną i nie ogranicza możliwości państw członkowskich do

regulowania problematyki bezpieczeństwa teleinformatycznego administracji publicznej, a także objęcia zakresem większej liczby podmiotów. To zależy od państw członkowskich.

Zakres podmiotowy dyrektywy NIS został ujęty w dwóch załącznikach nr II i III. Załącznik II dotyczy operatorów usług kluczowych, a załącznik III reguluje dostawców usług cyfrowych. Operatorów wskazanych w każdym z załączników obowiązywać będą inne wymagania. W przypadku dostawców usług cyfrowych (załącznik III) obowiązywać będzie łagodniejsze i reaktywne podejście obejmujące działania nadzorcze *ex post*, tzn. po zaistnieniu incydentu i tylko przez to państwo, na którego terenie dostawca usługi ma swoją siedzibę. Tym samym podmioty z załącznika III nie będą podlegały ani opisanemu wcześniej procesowi identyfikacji, ani raportowania, jak w przypadku operatorów usług kluczowych. Takie podejście jest spowodowane międzynarodowym wymiarem operatorów dostarczających usługi cyfrowe, a tym samym obawą przed fragmentaryzacją jednolitego rynku cyfrowego UE. W wyniku negocjacji ustalono, że regulacjami zostaną objęte serwisy zakupowe, wyszukiwarki internetowe oraz usługi chmury obliczeniowej. Dyrektywa nie dotyczy bezpośrednio usług administracji publicznej, o ile nie są to usługi kluczowe wymienione w dyrektywie.

W zakresie I filaru każde państwo członkowskie było zobligowane do ustanowienia organów właściwych ds. bezpieczeństwa sieci i informacji, odpowiedzialnych za monitorowanie stosowania jej przepisów w sektorach objętych jej zakresem[821]. Filar II dyrektywy obejmuje współpracę między państwami członkowskimi. Ponadto w przypadku ustanowienia wielu organów właściwych każde państwo członkowskie musiało ustanowić Pojedynczy Punkt Kontaktowy (PPK)[822]. III filar dyrektywy to zobowiązania w zakresie bezpieczeństwa sieci i informacji, które są różne w zależności od załącznika. Operatorzy usług kluczowych są zobligowani do dokonania oceny zagrożeń cyberbezpieczeństwa, na jakie są narażeni, oraz do przyjęcia odpowiednich i proporcjonalnych środków mających na celu zapewnienie bezpieczeństwa sieci i informacji. Podmioty te mają obowiązek zgłaszania właściwym organom wszelkich incydentów poważnie zagrażających ich sieciom i systemom

informatycznym, mogących znacząco zakłócić ciągłość działania kluczowych usług (obowiązkowe raportowanie). Raportowaniu podlegają incydenty o „znaczącym wpływie na ciągłość działania operatorów", co *de facto* oznacza, że progi raportowania określą państwa członkowskie w procesie implementacji. Podmioty załącznika III będą natomiast objęte regulacją reaktywnym nadzorem *ex post*.

Ostatnią wymaganą przez dyrektywę instytucją jest CSIRT obejmujący cały zakres podmiotowy regulacji. Państwa członkowskie mogły wskazać kilka CSIRT, mogły także wskazać jeden, np. w obrębie organu właściwego. Dyrektywa zachowuje dużą elastyczność, jeżeli chodzi o wewnętrzne struktury systemu cyberbezpieczeństwa. Oznacza to, że państwa członkowskie mogą wyznaczyć jeden CSIRT narodowy dla całego kraju, kilka CSIRT poziomu narodowego, bądź zbudować sieć CSIRT sektorowych.

Specyfika uregulowania dostawców usług cyfrowych polega na tym, że zainteresowany właściwy organ powinien podejmować działania wyłącznie wtedy, gdy otrzymał dowód, np. od samego dostawcy usług cyfrowych, innego właściwego organu, w tym właściwego organu innego państwa członkowskiego, lub od użytkownika usługi, że dostawca usług cyfrowych nie spełnia wymogów niniejszej dyrektywy, w szczególności w wyniku wystąpienia incydentu. Właściwy organ nie powinien mieć ogólnego obowiązku nadzorowania dostawców usług cyfrowych[823].

Dyrektywa nałożyła na państwa członkowskie obowiązek przyjęcia narodowej strategii bezpieczeństwa sieci i informacji, w której zostaną określone m.in. narodowe cele i priorytety w dziedzinie cyberbezpieczeństwa, role i obowiązki organów administracji publicznej w procesie osiągania wyznaczonych celów, zasady współpracy sektorów publicznego i prywatnego oraz krajowa analiza ryzyka i zadania w zakresie edukacji na rzecz cyberbezpieczeństwa.

Jej przepisy umożliwiają stworzenie zarówno scentralizowanego systemu na poziomie krajowym, jak i podzielenie kompetencji między różne podmioty wymieniające informacje oparte na mechanizmach współpracy. Dyrektywa zobowiązuje także wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu państwowych zdolności w dziedzinie bezpieczeństwa

teleinformatycznego, daje organom publicznym konkretne narzędzie do przeciwdziałania i reakcji na incydenty w cyberprzestrzeni. Jest to możliwe m.in. dzięki nałożonym obowiązkom raportowania poprzez przygotowanie krajowych strategii, skoordynowanie przepływu informacji czy zinstytucjonalizowanie współpracy CSIRT.

Przechodząc do analizy przypadku Polski, należy zaznaczyć, że w naszym kraju funkcjonują różne zespoły CSIRT, jednak tylko trzy działają od lat w ramach swojej właściwości na poziomie państwowym[824]. Zamiast tworzyć nowe podmioty, ustawa nadała określone zadania już istniejącym, które w ramach swojej działalności zajmują się reagowaniem na incydenty komputerowe.

Zgodnie z art. 1 ustawy i art. 1 dyrektywy 2016/1148 nie ma ona zastosowania wobec przedsiębiorców telekomunikacyjnych i dostawców usług zaufania, którzy zostali już objęci europejskimi i krajowymi wymaganiami sektorowymi z zakresu cyberbezpieczeństwa[825]. W przepisach ogólnych, szczególnie art. 2 ustawy, określono zakres regulacji, słowniczek pojęć ustawowych, katalog podmiotów tworzących krajowy system cyberbezpieczeństwa oraz cele projektowanej ustawy. Ustawa określa organizację polskiego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy, zakres oraz tryb stanowienia *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej*[826].

Należy również zauważyć, że zgodnie z art. 288 TL[827] transpozycja przepisów wprost co do dyrektywy odnoszącej się do prawa krajowego nie jest rozwiązaniem przyjętym przez ustawodawcę unijnego. Priorytetem jest spójność krajowego systemu prawa z prawem unijnym.

Zapisana w dyrektywie NIS definicja bezpieczeństwa informacji rozszerzyła trzy podstawowe atrybuty (tzn. poufność, integralność i dostępność) o czwarty – autentyczność, czyli właściwość polegającą na tym, że podmiot jest tym, za kogo się podaje[828]. Ustawa wprowadza pojęcie sektorowego zespołu cyberbezpieczeństwa[829], a więc zespołu ustanowionego przez organ właściwy dla danego sektora lub podsektora wymienionego w załączniku do ustawy, odpowiedzialnego

za obsługę lub wsparcie obsługi incydentów w danym sektorze lub podsektorze.

Polski ustawodawca zdefiniował cyberbezpieczeństwo w art. 2 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa jako odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne. Jest to definicja oparta na definicji „bezpieczeństwa sieci i systemów informatycznych" z dyrektywy 2016/1148 przy uwzględnieniu zmian niektórych pojęć, np. systemu informacyjnego.

Ustawa wprowadza kilka kategorii incydentów, które różnią się w zależności rodzaju podmiotu je zgłaszającego i stopnia jego oddziaływania (progów). Incydent poważny[830], zgłaszany przez operatora usług kluczowych, jest związany z poważnym obniżeniem jakości lub przerwaniem ciągłości działania świadczonej usługi kluczowej, a incydent istotny[831] ma istotny wpływ na świadczenie usługi cyfrowej. Incydent w podmiocie publicznym[832] nie jest uzależniony od progu oddziaływania, ale dotyczy wszystkich zdarzeń, które powodują lub mogą spowodować obniżenie jakości bądź przerwanie realizacji zadania publicznego. Przewidziano również incydenty krytyczne[833] skutkujące znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów gospodarczych, działania instytucji publicznych[834]. Definicje incydentu w podmiocie publicznym i incydentu krytycznego nie wynikają z dyrektywy NIS, ale były konieczne dla uzupełnienia systemu zgłaszania incydentów.

Definicja systemu informacyjnego opiera się na definicji systemu teleinformatycznego, zaczerpniętej z art. 3 obowiązującej ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[835] oraz danych w postaci elektronicznej przetwarzanych w tych systemach. Systemem teleinformatycznym jest zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy – Prawo telekomunikacyjne.

Wprowadzając zgodnie z wymogami dyrektywy 2016/1148 definicję systemów informacyjnych, która dodatkowo obejmuje przetwarzane w systemie teleinformatycznym dane w postaci elektronicznej, ustawodawca przyjął podejście, że pojęcie systemu informacyjnego uwzględnia komponent sprzętu, oprogramowania, sieci oraz danych i jest rozumiane z punktu widzenia realizacji usług kluczowych i usług cyfrowych. Przyjęte definicje oznaczają również, że ustawa obejmuje swoim zakresem zarówno systemy informatyczne (IT – *Information Technology*), systemy sterowania przemysłowego (OT –*Operational Technology*), jak i infrastrukturę wirtualną (informacyjną), np. zbiory informacji z baz danych. Przesłanką do objęcia wymaganiami z zakresu cyberbezpieczeństwa mogą być ustalone rozporządzeniem Rady Ministrów progi istotności incydentu we wspomnianych systemach informacyjnych.

Przyjęto również definicję obsługi incydentu[836], wskazując na następujące czynności operacyjne i techniczne, będące etapami obsługi incydentu:

- wykrywanie – punkt startowy procesu obsługi, każdy incydent ma zostać wykryty, konieczna jest tu aktywność operatora, a zaniechanie działalności na rzecz tego etapu będzie oznaczać brak realizacji obowiązku ustawowego;
- rejestrowanie – niezbędne jest prowadzenie rejestru incydentów, które miały miejsce w danym systemie;
- analizowanie – operator musi dokonać (wstępnej) analizy incydentu;
- klasyfikowanie – konieczne jest dokonanie klasyfikacji incydentu, ustawa nie wskazuje przyjętego modelu klasyfikacji, ale przyjęcie tego samego modelu co zespół CSIRT wspierający obsługę przyspieszy uzyskanie wsparcia;
- priorytetyzacja – oprócz skategoryzowania incydentu operator musi być w stanie określić jego priorytet, czy jest to incydent do obsługi w pierwszej kolejności, czy jest możliwe jego obejście i zajęcie się pilniejszym problemem;
- podejmowanie działań naprawczych, operator ma możliwość naprawienia szkód wyrządzonych przez incydent;

- ograniczenie skutków incydentu – operator jest w stanie przywrócić stan normalnego działania.

Obsługa incydentu jest obowiązkiem każdego operatora, dostawcy i podmiotu publicznego. Nie chodzi tu tylko o incydenty poważne, ale również zwykłe. Z kolei zarządzanie incydentem[837] jest terminem szerszym i poza obsługą obejmuje również:

- wyszukiwania powiązań między incydentami – wynajdywania powiązań między poszczególnymi elementami łańcuchu niszczenia intruza (*kill chain)* przez wykrycie zależności między np. rodzajem ataku a sposobem dostarczenia złośliwego oprogramowania, czy też między różnymi incydentami, np. czy korzystają z tej samej podatności, co wskazuje na pilną konieczność jej likwidacji;
- usuwania przyczyn wystąpienia incydentów – likwidacji podatności istniejących w posiadanym oprogramowaniu, podejmowanie czynności zmniejszających ryzyko wystąpienia incydentu w przyszłości, usuwanie wykrytych podatności;
- opracowywania wniosków wynikających z obsługi incydentu – przejrzenie i ocena swojej działalności podczas obsługi incydentu, przejrzenie oprogramowania, procesów i procedur w zakresie bezpieczeństwa w celu poprawy poziomu bezpieczeństwa w przyszłości.

Ustawa wprowadziła pojęcie podatności[838], czyli właściwości systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa[839], które z kolei zostało zdefiniowane jako potencjalna przyczyna incydentu. Przyjmując te definicje, opierano się na istniejących normach i standardach bezpieczeństwa teleinformatycznego.

Artykuł 5 wprowadza do polskiego porządku prawnego nową kategorię podmiotów, czyli operatora usługi kluczowej. Ustawodawca wzoruje się na definicji z dyrektywy 2016/1148 i określił nim podmiot spełniający następujące przesłanki:

- będzie jednym z podmiotów wymienionych w załączniku do ustawy;

- będzie świadczył usługę kluczową wymienioną w wykazie usług kluczowych;
- świadczenie tej usługi będzie zależeć od systemów informacyjnych;
- incydent miałby istotny skutek zakłócający dla jej świadczenia.

Wobec takiego podmiotu organ właściwy będzie mógł wydać decyzję administracyjną o uznaniu za operatora usługi kluczowej.

Wykaz usług kluczowych i progi istotności skutku zakłócającego dla świadczenia tych usług będą określone rozporządzeniem Rady Ministrów (art. 6 ustawy). Ustawodawca przewidział również tryb decyzji administracyjnych w przypadku zaprzestania spełniania przez podmiot warunków dla operatora usługi kluczowej (art. 5 ust. 6). Stroną praw i obowiązków określonych w ustawie jest operator usługi kluczowej. Artykuł 7 ustawy zobowiązuje ministra właściwego ds. informatyzacji do prowadzenia wykazu operatorów usług kluczowych. Wykaz ten zostanie utworzony z uwzględnieniem podziału na sektory, podsektory i rodzaje podmiotów, który wprowadza ustawa. Wpis do wykazu lub wykreślenie z niego ma charakter deklaratoryjny i będzie czynnością materialno-techniczną, realizowaną na podstawie decyzji administracyjnych organów właściwych, w zakresie identyfikacji operatorów usług kluczowych we właściwych sektorach. Przepis ten określa również tryb udostępniania informacji i katalog podmiotów, którym będą udostępniane informacje z wykazu.

Dyrektywa 2016/1148 wyznacza poziom harmonizacji minimalnej i dopuszcza możliwość ustanowienia szerszego katalogu grupy podmiotów, z których w procedurze administracyjnej mógłby zostać wyłoniony operator usługi kluczowej. W wyniku konsultacji z potencjalnymi organami właściwymi ustawodawca objął zakresem ustawy wszystkie kategorie podmiotów wymienionych w załączniku II do dyrektywy 2016/1148 oraz inne kategorie podmiotów, które nie zostały ujęte w załączniku nr 1 do ustawy. Należy przy tym dodać, że wskazanie danej kategorii[840] podmiotu ma służyć wskazaniu potencjalnych podmiotów, wobec których może zostać wydana obecnie bądź w przyszłości decyzja o uznaniu za operatora usługi

kluczowej, ale nie oznacza to automatyzmu uznania takiego podmiotu za operatora usługi kluczowej.

W art. 8 zostały określone obowiązki operatorów usług kluczowych w zakresie stosowania zabezpieczeń systemów informacyjnych służących do świadczenia usług kluczowych, szacowania i zarządzania ryzykiem oraz realizowania procedur dotyczących zarządzania incydentem. Operatorzy są odpowiedzialni za zapewnienie bezpieczeństwa świadczonych usług kluczowych oraz ich ciągłości. Ich głównym obowiązkiem jest wdrożenie systemu zarządzania bezpieczeństwem, a w pkt 2 wskazano minimalny zakres, jaki ma on obejmować. Na system ten składają się zabezpieczenia dotyczące bezpieczeństwa fizycznego, zarządzania ciągłością działania, obsługi i zarządzania incydentem, zarządzania podatnościami, objęcia systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym oraz stosowania środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.

Artykuł 9 zawiera zamknięty katalog obowiązków o charakterze organizacyjnym, które musi realizować operator usług kluczowych. Ustawodawca wymienia wśród nich wyznaczenie podmiotu[841] odpowiedzialnego za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz zapewnienie użytkownikom usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczeń, czyli budowania świadomości użytkowników.

Z uwagi na powszechny dostęp do rejestrów przedsiębiorców zdjęto z operatorów usług kluczowych obowiązek aktualizacji danych w wykazie. Ciężar aktualizacji tych danych będzie spoczywał na organach, które będą badały sytuację w sektorze. Jednak ze względu na fakt, że niektóre informacje nie są dostępne w publicznych rejestrach (np. informacja, w jakich państwach członkowskich Unii Europejskiej podmiot został uznany za operatora usługi kluczowej oraz datę zakończenia świadczenia usługi kluczowej) nałożono na operatora obowiązek aktualizacji tych danych.

Artykuł 10 precyzuje obowiązki operatorów usług kluczowych związane z opracowywaniem i ustanowieniem nadzoru nad

dokumentacją dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych. Upoważnienia do wydania przez Radę Ministrów rozporządzenia określającego rodzaje tworzonej dokumentacji. Przepis zawiera wyłączenie w zakresie realizacji tego obowiązku przez właścicieli, posiadaczy samoistnych lub zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym, którzy realizują obowiązki tego typu na podstawie tej ustawy. Rozwiązanie to ogranicza tym samym obowiązki administracyjne tworzenia dokumentacji dotyczącej cyberbezpieczeństwa, o ile dany operator usług kluczowych został już objęty obowiązkami, o których mowa w przepisach o zarządzaniu kryzysowym, i ma zatwierdzony plan ochrony infrastruktury krytycznej.

Na operatorów usług kluczowych zostały nałożone obowiązki związane ze zgłaszaniem i obsługą incydentu (art. 11 ustawy). Operatorzy będą zobowiązani do identyfikacji incydentu, jego rejestracji oraz klasyfikacji na podstawie progów uznawania incydentu za poważny. Przepisy nakładają obowiązki zgłaszania incydentów poważnych niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia. Przewidziana jest elektroniczna forma zgłaszania incydentu, która ma zostać określona przez CSIRT (art. 31 ustawy). Podstawowym założeniem ustawodawcy jest jak najszybsze zawiadomienie właściwego CSIRT. Samo zgłoszenie miałoby charakter inicjujący dalsze postępowanie z obsługą incydentu, ma także ograniczyć jego potencjalne skutki wobec innych podmiotów tworzących krajowy system cyberbezpieczeństwa. W procesie obsługi incydentu operator będzie zobowiązany do współpracy z odpowiednim CSIRT, a w razie potrzeby ma zapewnić dostęp do informacji o rejestrowanych incydentach oraz poinformować właściwy CSIRT o usunięciu podatności, które doprowadziły lub mogłyby doprowadzić do poważnego incydentu.

Przepisy rozdziału 5 ustawy definiują obowiązki podmiotów publicznych objętych zakresem ustawy. Podmioty publiczne objęte wymogami z zakresu cyberbezpieczeństwa będą zobowiązane do

wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (art. 21) oraz udostępniania wiedzy na temat zagrożeń cyberbezpieczeństwa i stosowania odpowiednich zabezpieczeń przed tymi zagrożeniami (art. 22 ust. 1 pkt 4).

Warto zaznaczyć, że mimo wprowadzenia dyrektywy NIS w Polsce nie ma nadal ustawowych przepisów wskazujących zakres kompetencji organów w obszarze cyberbezpieczeństwa, choć takie założenia zostały przyjęte w obecnym *Programie Strategii Cyberbezpieczeństwa RP*. Nie należy jednocześnie zapominać o ciągłym monitorowaniu cyberprzestrzeni, mimo że podjęcie decyzji o wprowadzeniu danego rodzaju stanu nadzwyczajnego będzie zależeć od oceny stopnia zagrożenia bezpieczeństwa państwa. Kwestią bezsporną pozostaje objęcie ochroną cyberprzestrzeni ze względu na jej wpływ na bezpieczeństwo narodowe, a w szczególności finanse publiczne państwa. Z kolei rzeczą problematyczną pozostaje ocena zagrożenia cyberprzestrzeni.

Ustawa NIS zawiera regulacje, które wydają się wykraczać poza zakres spraw przekazanych do uregulowania w rozporządzeniu, zwłaszcza w zakresie, w jakim wskazują na skutki związane z wystąpieniem danego zdarzenia, np. incydent spowodował straty finansowe przekraczające 100 tys. zł albo skutkuje niemożnością prawidłowej realizacji procesu dostawy i świadczenia usługi na rzecz sektora energii. Należy zauważyć, że w następstwie zakwalifikowania na podstawie progów określonych w rozporządzeniu danego incydentu jako poważnego, operator usługi kluczowej jest obowiązany zawrzeć w zgłoszeniu incydentu poważnego skutki jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe, zgodnie z art. 12 ust. 1 pkt 1 lit. f ustawy o krajowym systemie cyberbezpieczeństwa.

Plan działań, będący załącznikiem do Krajowych Ram, zawiera zestawienie projektów szczegółowych realizowanych przez poszczególne resorty czy podmioty. Obejmuje działania o charakterze legislacyjnym, projekty związane z budową systemów informacyjnych służących bieżącemu zarządzaniu cyberbezpieczeństwem, projekty o charakterze organizacyjnym, np. ćwiczenia, treningi i testy, czy też

działania ciągłe związane z rozbudową polskiego potencjału technologicznego i dotyczące udziału Polski we współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa. W obszarze realizacji Krajowych Ram przygotowano i rozesłano do konsultacji do poszczególnych ministerstw projekt ustawy o krajowym systemie cyberbezpieczeństwa. Opracowana została koncepcja funkcjonalna projektu *Narodowa Platforma Cyberbezpieczeństwa*, w tym centralna warstwa analityczna, przeprowadzono ćwiczenia z zakresu cyberbezpieczeństwa CEREX, jak również we współpracy z Ministerstwem Rozwoju (od 2021 r. – Ministerstwo Rozwoju, Pracy i Technologii) rozpoczęto realizację projektu Cyberpark ENIGMA. Określono zadania pełnomocnika rządu ds. cyberbezpieczeństwa (nowego podmiotu zajmującego się koordynacją działań dotyczących zapewnienia cyberbezpieczeństwa w RP) oraz Kolegium ds. cyberbezpieczeństwa (organu opiniodawczo-doradczego w sprawach cyberbezpieczeństwa) w celu zapewnienia koordynacji realizacji zadań na poziomie rządowym.

Ustawa wprowadziła również pojęcie sektorowego zespołu cyberbezpieczeństwa, czyli zespołu ustanowionego przez organ właściwy dla danego sektora lub podsektora wymienionego w załączniku do ustawy, odpowiedzialnego za obsługę lub wsparcie obsługi incydentów w danym sektorze lub podsektorze. Sektorowe zespoły zostały uregulowane w art. 44 ustawy.

Jedną z wad jest brak precyzyjnych zasad funkcjonowania jednostek zależnych od organów państwowych funkcjonujących również na rynku komercyjnym, w tym m.in. brak ograniczeń prowadzenia działalności komercyjnej przez jednostki wykonujące zadania CSIRT w zakresie wynikającym z ustawy. W mojej ocenie podmiot pełniący funkcję CSIRT powinien realizować wyłącznie zadania o charakterze publicznym i niekomercyjnym. Jego funkcjonowanie na rynku konkurencyjnym budzi istotne wątpliwości, szczególnie w sytuacji gdy możliwość pozyskiwania (z mocy prawa) informacji od innych podmiotów stawia go w uprzywilejowanej pozycji rynkowej.

Kolejną wadą jest brak ograniczenia zakresu uprawnień nadzorczych organów wyłącznie do obszaru związanego bezpośrednio ze świadczeniem usług kluczowych.

Moje zastrzeżenia budzi przede wszystkim dualizm regulacji w zakresie przyjętej właściwości odnośnie do konkretnych systemów i usług teleinformatycznych. Nieuwzględnienie zasad właściwości organów wynikających z ustawy o zarządzaniu kryzysowym może doprowadzić do sytuacji, w której kwalifikacji tych samych usług będą dokonywać różne podmioty. W przypadku uznania w obu ustawowych reżimach właściwości przez różne organy odnoszących się do tego samego systemu teleinformatycznego dojdzie do zakłócenia w systemie zapewniania bezpieczeństwa tych systemów.

Inną wadą są szerokie uprawnienia CSIRT umożliwiające żądanie od operatorów telekomunikacyjnych udostępnienia informacji dotyczących działalności oraz przyjętych rozwiązań organizacyjno-technicznych. Wprowadzenie takich rozwiązań z pominięciem analizy ryzyka i bez uwzględnienia zasady adekwatności stosowanych zabezpieczeń do zidentyfikowanych ryzyk może w istotnym zakresie ograniczać swobodę działalności gospodarczej, a jednocześnie obniżać efektywność prowadzonych działań w obszarze cyberbezpieczeństwa

Wadą jest również brak jednoznacznego i niebudzącego wątpliwości określenia odpowiedzialności za obsługę incydentu poważnego. Z jednej strony odpowiedzialność za obsługę incydentu spoczywa na operatorze, z drugiej – ustawa przewiduje wprost uprawnienia CSIRT w zakresie obsługi incydentów poważnych, nie wskazując przy tym zasad podejmowania decyzji przez CSIRT w zakresie incydentów, przyznając CSIRT pewne uprawnienia „władcze” wobec operatora. Tym samym CSIRT miałby możliwość ingerencji w działalność jednostkowego operatora z pominięciem jakiejkolwiek odpowiedzialności za działania podejmowane wobec operatora.

Warto również skrócić terminy reakcji przewidziane rozporządzeniem wykonawczym dotyczących sektora „Energia” z 30 minut do 15 minut w przypadku utraty kontroli nad systemami sterowania. Jest to podyktowane koniecznością jak najpilniejszego dotarcia przedmiotowej informacji do właściwych CSIRT ze względu na możliwe skutki przedmiotowego zdarzenia, w tym uzależnienie innych sektorów od dostaw energii.

Kolejnym uchybieniem jest brak jednego punktu zgłoszeń incydentów na poziomie krajowym, do którego byłoby można zgłaszać

incydenty, a przekierowanie incydentu według jego właściwości należałoby do podstawowych obowiązków tego punktu. Takie rozwiązanie wydaje się efektywniejsze niż zaproponowany dualistyczny, dość skomplikowany model zgłaszania poszczególnych kategorii incydentów w Polsce. Warto zauważyć, że liczba organów, do których przedsiębiorca powinien zgłaszać incydenty, w ostatnim okresie wraz ze stopniowym wprowadzaniem NIS znacząco wzrasta. Takie obowiązki istniały już w zakresie zgłoszeń do UKE, GIODO, Departamentu Informatyzacji. Od momentu wejścia w życie dyrektywy NIS taki obowiązek został wprowadzony dodatkowo wobec CSIRT NASK (odnośnie do incydentów istotnych przy usługach cyfrowych) oraz odpowiedniego CSIRT (dotyczących incydentów poważnych przy usługach kluczowych).

6.3 IMPLEMENTACJA POLITYKI CYBERBEZPIECZEŃSTWA W RFN

6.3.1. PODSTAWA PRAWNA POLITYKI CYBERBEZPIECZEŃSTWA

Niemcy są państwem, w którym bezpieczeństwo cybernetyczne postrzegane jest jako istotne dobro publiczne. Nie jest to temat poboczny, a rządzący zdają sobie sprawę z wymierności strat powodowanych przez zaniechania w dziedzinie cyberbezpieczeństwa. Od 2015 r. doszło do kilku skandali w omawianym obszarze, poczynając od kwestii szpiegostwa najwyższych urzędników państwowych ze strony USA, kończąc na kolejnych doniesieniach prasowych o zawirusowanych komputerach najważniejszych polityków[842]. Republika Federalna Niemiec jest narażona na ataki w cyberprzestrzeni w wysokim stopniu jako państwo opierające się na zaawansowanych technologiach i będące w sposób ponadprzeciętny zglobalizowane. Zgodnie z szacunkami z 2011 r. ponad 70% dużych

niemieckich przedsiębiorstw padło ofiarą cyberataku, a liczba i stopień złożoności takich incydentów są coraz wyższe[843].

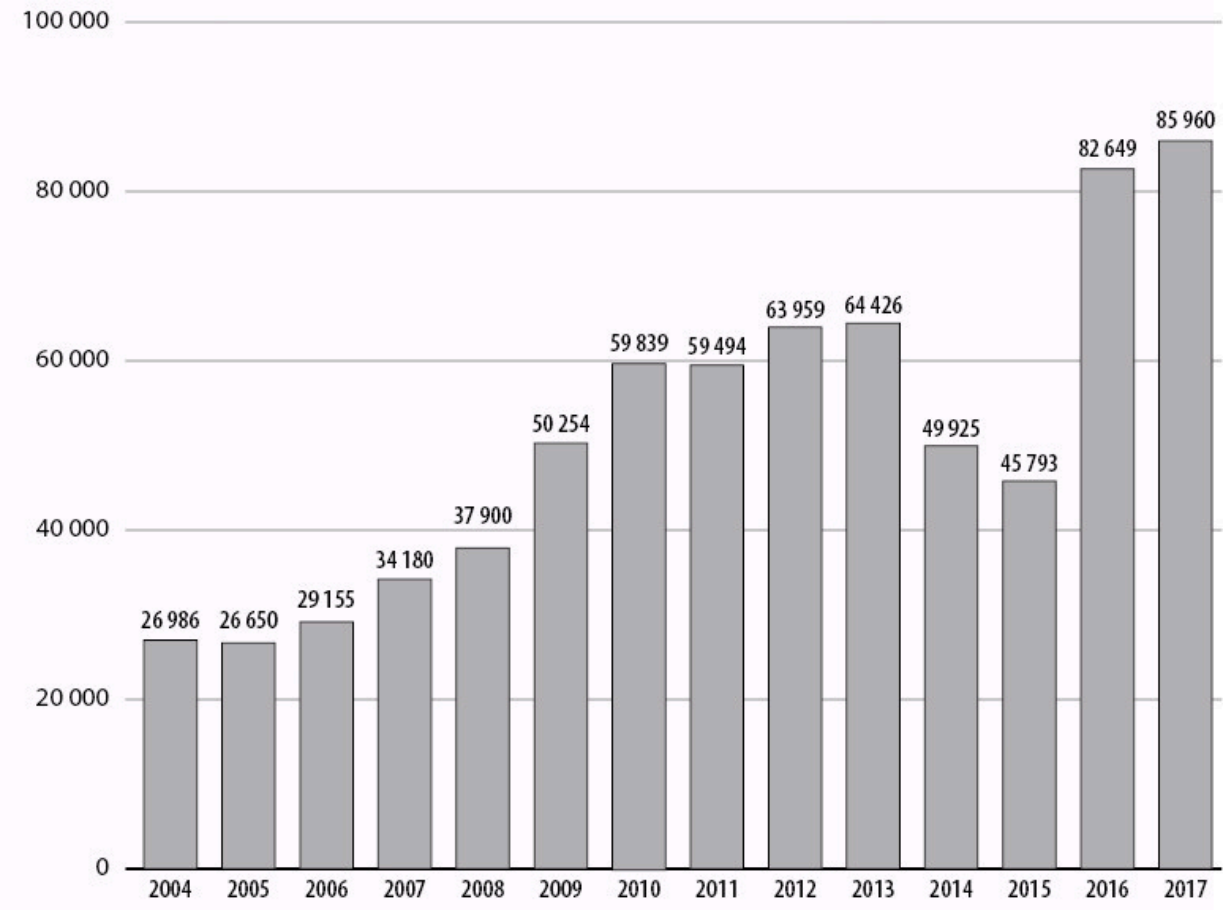
W Niemczech już kilka lat temu podjęto wysiłek przyjęcia i usystematyzowania polityki walki z cyberterroryzmem. Jednym z pierwszych aktów prawnych dotyczących cyberbezpieczeństwa był tzw. *Plan realizacji KRITIS – narodowy plan ochrony infrastruktury informacyjnej* (*Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen*) z 2007 r. opracowany przez Ministerstwo Spraw Wewnętrznych[844]. Skupia się on na ochronie infrastruktury krytycznej, a jego adresatami są przede wszystkim prywatne przedsiębiorstwa działające w wybranych obszarach, ważnych z punktu widzenia zapewniania dóbr publicznych. Plan zawiera rekomendacje rozwiązań podzielonych na trzy etapy[845]:

- prewencję, która dotyczy rozwiązań z zakresu m.in. organizacji bezpieczeństwa IT, utrzymania krytycznych procesów biznesowych, bezpieczeństwa w całym cyklu życia produktu, prowadzenia szkoleń itp.;
- reakcję, która dotyczy m.in. sposobów oceny sytuacji w zakresie bezpieczeństwa IT, mechanizmów ostrzegania, reakcji na kryzysy, protokołowania i monitoringu;
- rozwój dotyczący m.in. kształcenia w zakresie cyberbezpieczeństwa, prac R&D, percepcji interesów na poziomach krajowym i międzynarodowym.

Dokument dotyczy również sposobów komunikacji o zagrożeniach bezpieczeństwa cybernetycznego i zawiera mapę drogową bezpieczeństwa cybernetycznego z następującymi podpunktami: ćwiczenia na wypadek kryzysów, pożądane reakcje w wypadku kryzysu, sposoby utrzymania działalności infrastruktury krytycznej w przypadku ataku, plany współpracy na poziomach narodowym i międzynarodowym. Ponieważ postanowienia planu zostały zastąpione przez przyjęte później akty, jego szczegółowa analiza zostanie tutaj pominięta.

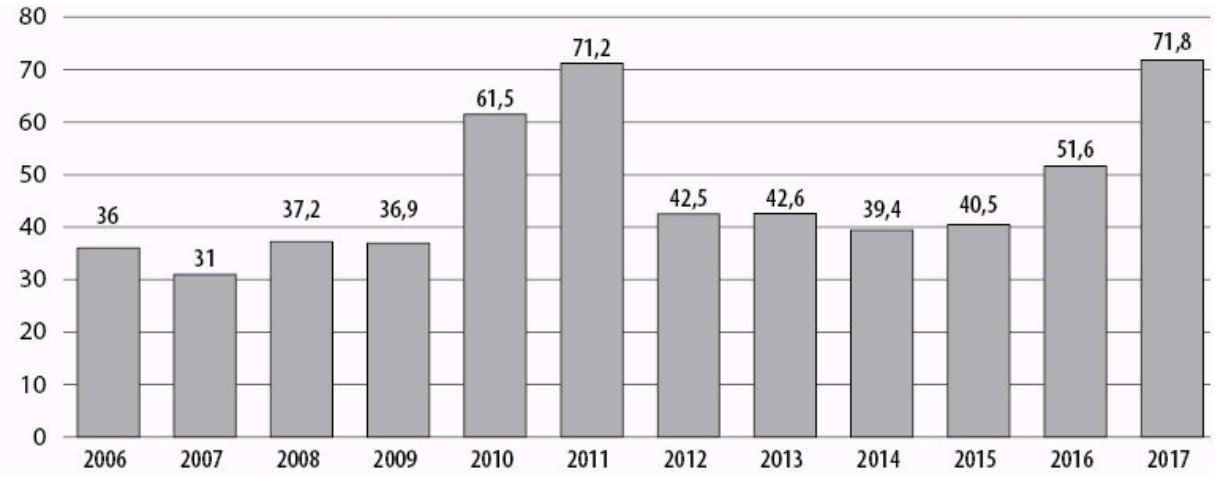
Na *rysunkach 7–8* zaprezentowano przypadki cyberprzestępczości odnotowanej w latach 2004–20017 na terenie Niemiec oraz szkody, jakie wyrządziła. W 2017 r. w Niemczech miało miejsce 85 960

incydentów związanych z cyberprzestępczością. Obszar obejmuje przestępstwa związane z oszustwami komputerowymi, nadużyciami w korzystaniu z usług telekomunikacyjnych, fałszowaniem dowodów, oszustwami w transakcjach prawnych w przetwarzaniu danych, modyfikacją danych lub sabotażem komputerowym i szpiegowaniem, przejęciem danych, w tym działania przygotowawcze. W ten sposób cyberprzestępczość obejmuje wszystkie przestępstwa popełniane przy użyciu lub przeciwko technologii informacyjnej i komunikacyjnej.



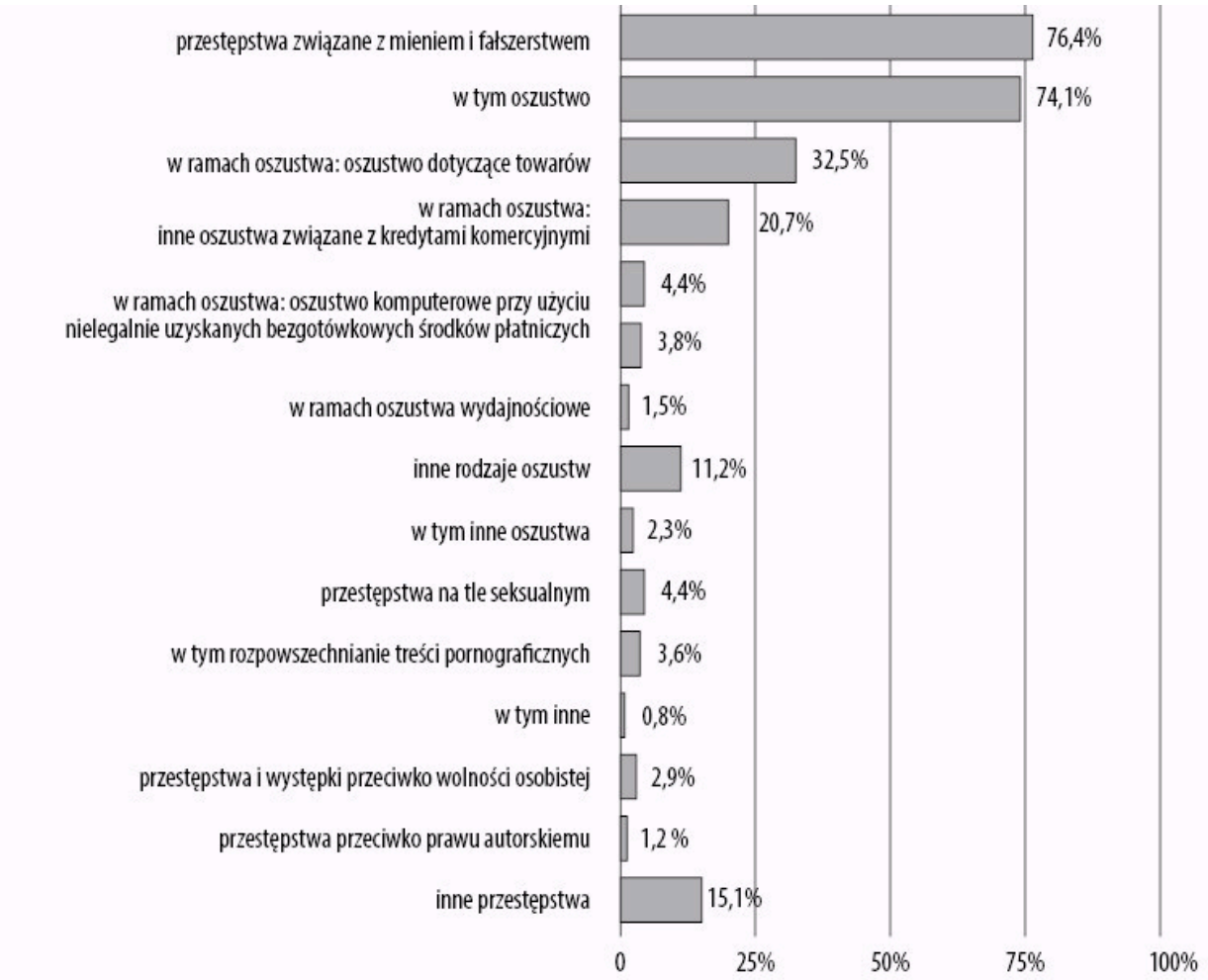
RYSUNEK 6.7 Zarejestrowane przez policję przypadki cyberprzestępczości w Niemczech w latach 2004–2017

Źródło: https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalitaet-im-engeren-sinne-in-deutschland/ (dostęp: 23.07.2020).



RYSUNEK 6.8
Szkody spowodowane cyberprzestępczością w Niemczech w latach 2004–2017 (w mln euro)

Źródło: https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalitaet-im-engeren-sinne-in-deutschland/ (dostęp: 23.07.2020).



RYSUNEK 6.9 Odsetek cyberprzestępstw w Niemczech (styczeń 2019 r.)

Źródło: https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalitaet-im-engeren-sinne-in-deutschland/ (dostęp: 23.07.2020).

W 2009 r. opublikowano *Narodową Strategię Ochrony Infrastruktury Krytycznej* (*Nationale Strategie zum Schutz Kritischer Infrastrukturen*)[846] ponownie w ramach Ministerstwa Spraw Wewnętrznych. Dokument jest ogólny i w mojej opinii raczej nie spełnia wymogów prawdziwej strategii. Brak przede wszystkim mierzalnych i wyraźnie określonych celów. Dokument wylicza inicjatywy i pakiety środków przyjęte przez Niemcy w poprzednich latach w odniesieniu do bezpieczeństwa infrastruktury krytycznej. Są to m.in. wewnętrzne akty prawne, podpisane umowy międzynarodowe, ćwiczenia z zarządzania

kryzysowego LÜKEX (*Länderübergreifende Krisenmanagement Exercise* – nie dotyczą jednak stricte bezpieczeństwa IT) oraz elementy programu *Badania dla bezpieczeństwa cywilnego* (*Forschung für die zivile Sicherheit*)[847]. Strategia zawiera również przykłady zagrożeń dla infrastruktury krytycznej, wśród których nie znalazły się jednak cyberataki.

Strategię cyberbezpieczeństwa dla Niemiec przyjęto 23 lutego 2011 r.[848] Jest to krótki i dosyć ogólny dokument, jedynie naświetlający podstawowe założenia polityki państwa oraz priorytetowe kierunki działań w omawianym obszarze. Mimo zwięzłości zawiera kilka konkretnych rozwiązań (już wdrożonych). Podobnie jak w przypadku generalnych założeń polityki bezpieczeństwa RFN, w wymiarze operacyjnym strategia stawia na wszechstronne podejście (*comprehensive approach*), którego głównymi elementami są zarówno w wymiarze krajowym, jak i międzynarodowym wymiana informacji i koordynacja.

Strategia Cyberbezpieczeństwa dla Niemiec z 2011 r. zdefiniowała cyberprzestrzeń w następujący sposób: „Cyberprzestrzeń jest wirtualną przestrzenią wszystkich systemów technologii informacyjnej powiązanych na poziomie danych w skali globalnej". Fundament cyberprzestrzeni stanowi Internet jako uniwersalna i powszechnie dostępna sieć oferująca połączenia oraz transport, która może być uzupełniania i rozszerzana dalej przez dowolną ilość dodatkowych sieci danych. Systemy IT działające w wyizolowanej przestrzeni wirtualnej nie stanowią części cyberprzestrzeni. Jak wynika wprost z ostatniego zdania definicji, systemy odłączone od globalnych zasobów cyberprzestrzeni (w praktyce od Internetu) nie wchodzą w skład cyberprzestrzeni niemieckiej.

Strategia określa główne obszary, na których powinien skupić się rząd federalny. Są to:

- ochrona krytycznych informacji i infrastruktury;
- zapewnienie bezpieczeństwa systemom IT w Niemczech;
- wzmocnienie bezpieczeństwa IT w administracji publicznej;
- efektywne zwalczanie przestępczości w cyberprzestrzeni;
- efektywna koordynacja działań na rzecz zapewnienia cyberbezpieczeństwa w Europie i na świecie;

- używanie godnych zaufania technologii informacyjnych;
- rozwijanie kadr w organach federalnych (weryfikacja już zatrudnionych zasobów oraz racjonalne planowanie);
- rozwój narzędzi odpowiedzi na cyberataki;
- utworzenie Narodowego Centrum Przeciwdziałania Cyberzagrożeniom (Nationales Cyber-Abwehrzentrum) i Narodowej Rady Cyberbezpieczeństwa (Nationaler Cyber-Sicherheitsrat).

Część tych zadań została zakreślona ogólnie, natomiast strategia zawiera również bardziej szczegółowe zalecenia. Przykładowo, w odniesieniu do punktu dotyczącego wzmocnienia bezpieczeństwa IT w administracji publicznej autorzy dokumentu zakładają utworzenie wspólnej, uniwersalnej infrastruktury sieciowej dla administracji federalnej[849]. W zakresie prawa międzynarodowego przewiduje się podjęcie wysiłku legislacyjnego, aby zharmonizować niemieckie prawo karne z zaleceniami określonymi w *Konwencji Rady Europy o cyberprzestępczości* nr 185105. Niemcy rozważą również zasadność wypracowania analogicznych rozwiązań w ramach Narodów Zjednoczonych[850].

Na poziomie europejskim strategia zakłada wsparcie dla „umiarkowanego zwiększenia" mandatu Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA)[851]. Dokument postuluje prace nad zacieśnieniem współpracy międzynarodowej w omawianej dziedzinie na forum takich instytucji, jak: ONZ, OBWE, Rada Europy, OECD, G7/8 i NATO. Jednym z pomysłów jest stworzenie kodeksu postępowania państw w cyberprzestrzeni (nazwanego *cyberkodem*), który mógłby zawierać również środki budowy zaufania – rozwiązanie znane z bardziej tradycyjnych traktatów o współpracy wojskowej i wymianie informacji. Wychodząc z założenia, że NATO jest podstawą bezpieczeństwa transatlantyckiego, strategia opowiada się za budowaniem cyberkompetencji sojuszu, m.in. ustanowieniem jednakowych standardów bezpieczeństwa dla cywilnej infrastruktury krytycznej. Warto zaznaczyć, że Niemcy regularnie biorą udział w cyberćwiczeniach NATO *Locked Shields*.

Strategia cyberbezpieczeństwa zawiera również słownik definicji, w której cyberatak zdefiniowano jak atak IT w cyberprzestrzeni skierowany przeciw jednemu lub wielu systemom IT, mający na celu zmniejszenie bezpieczeństwa IT przez naruszenie prywatności, integralności lub dostępności danych. Jeśli cyberatak jest przeprowadzany lub zarządzany przez zagraniczne służby wywiadowcze, jest aktem cyberszpiegostwa. Cyberatak, który ma na celu osłabienie integralności lub dostępności systemów IT, jest aktem cybersabotażu. W mojej opinii te definicje są dosyć wąsko lub nieprecyzyjnie zakreślone. Zawierają również listę obszarów infrastruktury krytycznej na poziomie federalnym. Są to takie organizacje lub instytucje, które mają podstawowe znaczenie dla społeczeństwa, a ich brak lub uszkodzenie mogłoby doprowadzić do powstania wąskich gardeł zaopatrzeniowych, istotnych zakłóceń bezpieczeństwa publicznego lub innych dramatycznych konsekwencji. Należą do nich następujące sektory:

- energia,
- technologia informacyjna i telekomunikacja,
- transport,
- zdrowie,
- woda,
- żywność,
- sektor finansowy i ubezpieczeń,
- państwo i administracja,
- media i kultura.

W listopadzie 2016 r. opublikowano kolejną *Strategię cyberbezpieczeństwa dla Niemiec* (*Cyber-Sicherheitsstrategie für Deutschland 2016*)[852] będącą kontynuacją poprzedniej. Nowy dokument określa ramy strategiczne działalności rządu federalnego z odniesieniami do cyberbezpieczeństwa. Wynika to z faktu, że wiele środków przewidzianych w poprzednim planie zostały już wdrożonych, np. powołano Narodowe Centrum Przeciwdziałania Cyberzagrożeniom oraz stworzono platformę dla strategicznej i operacyjnej wymiany między organami z cyberbezpieczeństwa, będącą punktem wymiany polityki i biznesu. Narodowe Centrum

Przeciwdziałania Cyberzagrożeniom stało się ważnym składnikiem różnych koncepcji strategicznych i rządowych. Zgodnie z wytycznymi nowej strategii rząd federalny RFN musiał położyć nacisk na cyberpolitykę w czterech obszarach:

- stworzenie bezpiecznych i autonomicznych podstaw prawnych do działania w środowisku cyfrowym;
- stworzenie wspólnych programów w zakresie cyberbezpieczeństwa państwa i gospodarki;
- wydajne i trwałe zapewnienie bezpieczeństwa systemom IT w Niemczech;
- aktywna i efektywna koordynacja działań na rzecz zapewnienia cyberbezpieczeństwa Niemiec w Europie i na świecie.

Kolejnym istotnym elementem legislacji w dziedzinie cyberbezpieczeństwa jest ustawa z 17 lipca 2015 r. o zwiększeniu bezpieczeństwa systemów technologii informacyjnych (ustawa o bezpieczeństwie IT)[853]. Zawiera ona innowacyjne rozwiązania w zakresie bezpieczeństwa IT zarówno na poziomie państwowym, jak dla i podmiotów prywatnych (zwanych w ustawie operatorami).

Zgodnie z § 3 ustawy dotyczy ona działalności podmiotów z obszaru infrastruktury krytycznej i wprowadza pakiet obowiązków. Obejmują one:

- wdrożenie środków ochrony systemów IT pod rygorem otrzymania grzywny w wysokości do 100 tys. euro w ciągu dwóch lat od wejścia w życie aktów wykonawczych do ustawy, które będą zawierały szczegóły dotyczące tych środków w zakresie każdego sektora infrastruktury krytycznej[854];
- regularną (nie rzadziej niż raz na dwa lata) kontrolę spełnienia standardów ochrony cybernetycznej, działania dopuszczalne w tym zakresie to m.in. audyty bezpieczeństwa lub odnawianie certyfikatów, operatorzy będą musieli przekładać sprawozdania z kontroli do BSI, który będzie mógł wnioskować o dalsze informacje lub podjęcie konkretnych środków;
- wyznaczenie osoby do kontaktu z BSI;
- natychmiastowe poinformowanie BSI o podejrzeniu cyberataku zdefiniowanego jako istotne zakłócenie dostępności,

integralności, autentyczności i poufności systemów IT, ich komponentów i procesów, które może doprowadzić lub doprowadziło do awarii lub upośledzenia funkcjonowania infrastruktury krytycznej.

Zgodnie z § 8a ust. 2 omawianej ustawy operatorzy infrastruktury krytycznej muszą przynajmniej raz na dwa lata dowieść implementacji i stosowania środków ochrony systemów IT. Taki dowód może polegać na przeprowadzeniu audytu IT lub uzyskaniu bądź odnowieniu odpowiedniego certyfikatu. Wymagania dotyczące poszczególnych sektorów zostaną określone w aktach wykonawczych do ustawy.

Specjalne obowiązki nałożono na operatorów telekomunikacyjnych – w myśl § 8c ustawy. Muszą oni informować klientów o przypadkach ataków na ich łącza, np. atakach typu *botnet*[855], oraz przechowywać dane o ruchu w sieci do celów dochodzeniowych przez 6 miesięcy. Istnieją zwolnienia z tych obowiązków, m.in. małe przedsiębiorstwa nie będą musiały wdrażać środków ochrony systemów IT, podobnie jak te podmioty, które zostały zobowiązane do implementacji takich lub podobnych środków na mocy oddzielnych ustaw (np. elektrownie).

Według przewidywań rządu RFN omawiany reżim powinien objąć nie więcej niż 2 tys. operatorów infrastruktury krytycznej. Krytycy ustawy wskazują na wysokie koszty dostosowania gospodarki do nowych standardów – prywatne szacunki oscylują wokół 1,1 mld euro rocznie. Nie podoba się również prawo operatorów telekomunikacyjnych do przechowywania informacji o działaniach ich klientów w sieci[856]. W ustawie nie określono również jasno, jakiego typu zdarzenia podlegają obowiązkowi zgłoszenia do BSI – cyberataki przyjmują różne formy i nie wszystkie stanowią istotne zagrożenie. Sektor prywatny wskazywał również obawy o utratę zaufania klientów, gdyby informacje o ataku przedostały się do wiadomości publicznej.

Zgodnie z art. 6 ustawy o telekomunikacji (TKG)[857] dostawca usługi, inaczej usługodawca (*Diensteanbieter*) oznacza osobę, która w pełni lub częściowo komercyjnie świadczy usługi telekomunikacyjne lub uczestniczy w świadczeniu takich usług. Ustawa przewiduje uchwalenie wielu aktów wykonawczych, które zostaną pogrupowane

zgodnie z poszczególnymi sektorami infrastruktury krytycznej. W połowie 2015 r. niemiecka prasa doniosła o istnieniu tajnej strategii Bundeswehry na wypadek wojny w cyberprzestrzeni. Dokument nie jest publicznie dostępny (choć jego prawdopodobna treść została zamieszczona w Internecie), jednak wydaje się zasadne przytoczenie choćby pobieżnie spekulacji prasowych. Według tygodnika „Der Spiegel" Ministerstwo Obrony Narodowej ma planować znaczny rozwój kompetencji Niemiec w zakresie prowadzenia cyberkonfliktu. Istniejące zasoby miałyby zostać jeszcze bardziej scentralizowane oraz dodatkowo rozwijane[858].

Według dokumentu rząd federalny liczy się w przyszłości z atakami na niemieckie systemy IT, w tym na kluczową infrastrukturę, które mogą nosić znamiona ataku zbrojnego. Takie ataki będą stanowić coraz większe zagrożenie dla Niemiec z uwagi na ich postępującą digitalizację, usieciowienie oraz poleganie na technologiach typu chmura obliczeniowa. Rozwijanie kompetencji armii w zakresie cyberbezpieczeństwa pozostaje w zgodzie z koncepcją „powiązanego bezpieczeństwa" (*vernetzte Sicherheit*), które jest rozwijane w Niemczech od wielu lat. W związku z tym Internet i inne platformy komunikacji miałyby być postrzegane przez armię jako taki sam obszar wojny, jak ląd, morze i powietrze. Dokument wskazuje, że zasoby armii – w tym jej platformy intranetowe i systemy obronne – muszą być chronione przed cyberatakami. Wspomina się również, że w przyszłości powinien zostać w Niemczech przeprowadzony audyt w zakresie zidentyfikowania i rozwijania kluczowych technologii IT[859].

Według doniesień dozwolone miałyby być również operacje ofensywne zgodne z ogólnymi regułami przeprowadzania operacji wojskowych. Przykładowo, podczas zagranicznych misji specjalne jednostki Bundeswehry mogłyby wspierać walczących na miejscu przez ograniczanie zdolności wroga do wykorzystywania Internetu i łączności mobilnej. Cyberataki na systemy przeciwnika miałyby cechować się wysoką skutecznością i precyzją, a tym samym w znaczący sposób uzupełniać tradycyjne zdolności Bundeswehry. W omawianym zakresie dokument planuje np. rozwijanie zdolności punktowego wydobywania informacji z systemów komunikacyjnych wroga. Wszelkie kompetencje powinny być zarządzane centralnie oraz

uprzednio rozwijane, aby było możliwe włączenie ich już na etapie planowania misji i operacji.

Armia powinna być w stanie efektywnie odpowiedzieć (tj. przerwać wrogą operację, zminimalizować jej skutki, jak najszybciej przywrócić stan wyjściowy oraz móc zidentyfikować agresora) na atak na niemieckie systemy IT, które nosiłyby znamiona ataku zbrojnego. Za tego typu zdarzenia w tajnym dokumencie uznano ataki na sieci komunikacyjne i transportowe.

Obecnie zgodnie z niemieckim prawem karane są następujące przestępstwa związane z cyberbezpieczeństwem:

- nielegalny dostęp do danych – art. 202a k.k.[860] – szpiegowanie danych;
- nielegalna interpretacja danych – 202b k.k.;
- ingerencja w dane – 303a k.k. – manipulowanie danymi;
- ingerencja w system – 303b k.k. – sabotaż komputerowy;
- niewłaściwe wykorzystanie urządzeń 202c k.k. – akty przygotowujące do szpiegostwa i wyłudzania informacji;
- fałszerstwo komputerowe – art. 267 k.k.;
- fałszowanie danych mających na celu dostarczenie dowodu – art. 269 k.k.;
- oszustwo – art. 263 k.k. oraz oszustwo komputerowe – art. 263a k.k.;
- przestępstwa związane z pornografią dziecięcą – 184b–c k.k. – dystrybucja, nabywanie i posiadanie pornografii dziecięcej i nieletniej;
- przestępstwa związane z naruszeniem praw autorskich i pokrewnych.

Artykuły 106–108b ustawy o prawie autorskim i prawach pokrewnych[861] przewidują odpowiedzialność prawną za naruszenie następujących dóbr prawnych:

- bezprawna eksploatacja dzieł chronionych prawem autorskim;
- naruszenie praw pokrewnych;
- bezprawne umieszczanie kogoś jako autora;
- bezprawna eksploatacja cudzego dzieła na skalę handlową;

- naruszenie środków technologicznych i informacyjnych dotyczących zarządzania prawami autorskimi.

Niemiecki kodeks karny przewiduje również odpowiedzialność karną za podżeganie, usiłowanie i pomocnictwo (art. 23. 26 i 27 k.k.). Odpowiedzialność osób prawnych jest przewidziana w drodze ustawy o odpowiedzialności pomiotów prawnych i dotyczy kar nakładanych na przedsiębiorstwa posiadające osobowość prawną i stowarzyszenia[862].

W 1986 r. do niemieckiego kodeksu karnego (*Strafgesetzbuch*) wprowadzono penalizację przestępstw komputerowych takich, jak hakerstwo, nieuprawniona zmiana danych, sabotaż komputerowy, oszustwo komputerowe oraz fałszerstwo komputerowe. Niemiecka ustawa karna, wprowadzając zasadę jurysdykcji terytorialnej, przewidziała wielomiejscowość popełnienia czynu. Uznano, że miejscem popełnienia przestępstwa jest zarówno miejsce działania sprawcy, jak i miejsce wystąpienia skutku czynu zabronionego. Przepisy ustawy stanowią ponadto, że podstawą wykonywania jurysdykcji jest zasada personalna odnosząca się do niemieckiego obywatela, który popełnił przestępstwo poza granicami państwa. Jak wskazuje Maciej Siwicki, zasadę terytorialną stosuje się wobec obywatela niemieckiego, który dopuścił się czynu przestępczego za pomocą mediów elektronicznych. Bez znaczenia pozostaje wówczas fakt, czy popełniając czyn, np. wprowadzając zakazane przez prawo niemieckie dane do Internetu, znajdował się na terytorium Niemiec, czy w państwie trzecim[863].

W niektórych przypadkach przestępstw komputerowych z łatwością można zastosować zasadę jurysdykcji terytorialnej lub zasadę wielomiejscowości popełnienia przestępstwa, a taka sytuacja wystąpi, gdy sprawca, przebywając na terytorium Niemiec, manipuluje danymi znajdującymi się na komputerze podlegającym pod jurysdykcję innego państwa, lub gdy sprawca z zagranicy niszczy dane na komputerze znajdującym się na terytorium Niemiec. Wówczas niemiecki wymiar sprawiedliwości będzie mógł zastosować własną jurysdykcję[864].

Sekcją 6 § 4–7 niemieckiego kodeksu karnego wprowadzono zasadę jurysdykcji uniwersalnej, zgodnie z którą prawo niemieckie stosuje się

do niewolnictwa, handlu narkotykami i rozpowszechniania pornografii dziecięcej niezależnie od miejsca popełnienia przestępstwa. Tę samą zasadę stosuje się wobec nieuprawnionego dostępu i ujawnienia tajemnicy handlowej przedsiębiorstw mających siedzibę na terytorium Niemiec oraz nielegalnego handlu organami (również za pomocą Internetu)[865].

Zastosowanie zasady terytorialności w odniesieniu do różnych rodzajów przestępstw, np. nienawiści czy pornografii w Internecie, oraz możliwości zastosowania prawa niemieckiego wzbudziły rozbieżności w doktrynie. Pierwszą było restrykcyjne podejście (*restrictive approach*), które zakłada, że sprawca, który np. umieścił treści pornograficzne na zagranicznym serwerze, rozesłał e-maile do niemieckich użytkowników lub zamieścił materiały o określonej treści w grupach dyskusyjnych zlokalizowanych na niemieckich serwerach, nie podlegałby jurysdykcji niemieckiej. Drugie szerokie podejście (*extensive approach*) zakłada, że miejscem popełnienia czynu są wszystkie miejsca, w których abstrakcyjnie mógł nastąpić ten czyn. Zwolennicy tej teorii stoją na stanowisku, że prawo niemieckie można będzie zastosować nie tylko w stosunku do osoby, która znajdując się w innym państwie, rozsyła e-mailem treści pornograficzne do Niemiec, ale również w stosunku do danych znajdujących się na zagranicznym serwerze, mimo że nie miałby on żadnego związku z Niemcami. Argumentują oni, że międzynarodowe oddziaływanie sieci komputerowych spowodowane rozwojem Internetu skutkuje pojawieniem się możliwości, że dane te mogą być dostępne na terytorium Niemiec. Zdaniem zwolenników szerokiego podejścia możliwość pojawienia się potencjalnego zagrożenia jest wystarczająca do zastosowania prawa niemieckiego. Inni teoretycy prawa wskazują na dodatkowe kryteria warunkujące możliwość zastosowania prawa niemieckiego. Będą to: świadomość domniemanego sprawcy, że udostępniane przez niego dane mogą być dostępne na terytorium Niemiec, działanie sprawcy w celu udostępnienia danych na terytorium Niemiec oraz język, w którym dane i treści są udostępnianie.

Problematyczna okazała się kwestia określenia jurysdykcji w sprawach internetowych, w których udostępnia się treści czy też

nawołuje do nienawiści na tle rasowym, propaguje partie i organizacje, które w swojej działalności głoszą treści zabronione lub nielegalne, lub pochwalają, umniejszają czy usprawiedliwiają czyny dokonane przez nazistów za pomocą treści zamieszczonych na zagranicznych serwerach. Punktem wyjścia do dalszych rozważań powinien być § 9 ust. 1 niemieckiego kodeksu karnego, który za miejsce przestępstwa uważa miejsce, w którym sprawca działał lub zaniechał działania, do którego był obowiązany, lub też gdzie skutek przestępczy nastąpił lub gdzie według zamiaru sprawcy miał nastąpić.

Zagadnienie udostępniania w cyberprzestrzeni treści o charakterze nazistowskim zostało podjęte w niemieckim orzecznictwie w sprawie Geralda Fredericka Tőbena, obywatela australijskiego, który za pomocą stworzonej przez siebie strony internetowej, umieszczonej na australijskim serwerze, publicznie znieważał osoby pochodzenia żydowskiego, rewidował i usprawiedliwiał zbrodnie nazistowskie oraz obrażał pamięć osób zmarłych. Czyny te są karane w prawie niemieckim. Maciej Siwicki wskazuje, że Bundesgerichtshof (Federalny Trybunał Sprawiedliwości – BGH) po rozpoznaniu sprawy stwierdził, że „adresatami jego rewizjonistycznych artykułów udostępnianych z wykorzystaniem Internetu, mimo że były one pisane w języku angielskim, byli obywatele Niemiec. […] Sąd podkreślił również, że oskarżony, zamieszczając informacje w Internecie, musiał liczyć się z ich ogólnodostępnością oraz z tym, że mogą być one bez problemów rozpowszechniane w Niemczech, stanowiąc realne zagrożenie dla porządku prawnego w tym państwie. […] Miejscem skutku przestępnego było terytorium Niemiec, ponieważ policjanci prowadzący dochodzenie zapoznali się z tymi treściami w czasie przeglądania zawartości strony internetowej”. BGH podkreślił również, że § 130 niemieckiego kodeksu karnego dotyczący znieważenia społeczności żydowskiej może w ograniczonym zakresie znaleźć zastosowanie zarówno do zagranicznych usługodawców świadczących usługi drogą elektroniczną, jak i użytkowników będących obywatelami innych państw, którzy udostępniają informacje zakazane przez prawo lub pomagają w dostępie do nich.

W RFN nielegalny dostęp do danych stanowi czyn karny zabroniony w myśl art. 202a k.k.[866] (szpiegowanie danych[867]). Przestępstwo to w

prawie RFN jest czynem umyślnym polegającym na bezprawnym dostępie do całości lub części systemu informatycznego. Przestępstwo musi zostać popełnione w wyniku naruszenia zabezpieczeń, z zamiarem pozyskania danych informatycznych lub innym nieuczciwym zamiarem lub w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym. Popełnia je każdy, „kto bezprawnie uzyska dla siebie lub innej osoby dane, które nie były dla niego przeznaczone i które były szczególnie chronione przed nieuprawnionym dostępem, jeśli obejdzie ochronę, podlega karze pozbawienia wolności nieprzekraczającej trzech lat lub grzywnie".

Z kolei nielegalna interpretacja danych jest przestępstwem zawartym w art. 202b k.k. W prawie niemieckim jest to czyn umyślny popełniony za pomocą urządzeń technicznych niepublicznych transmisji lub przechowywania danych informatycznych do, z, lub w ramach emisji elektronicznie lub magnetycznie lub w inny sposób, nieuchwytny od razu. Każdy, kto bezprawnie przechwytuje dane (art. 202a ust. 2), które nie są przeznaczone dla niego lub kogoś, za pomocą urządzeń technicznych z niepublicznych transmisji danych informatycznych, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne, podlega karze pozbawienia wolności nieprzekraczającej dwóch lat lub grzywny, chyba że przestępstwo podlega surowszej karze na podstawie innych przepisów.

Usiłowanie popełnienia przestępstw z art. 202a 202b k.k. w drodze „produkcji, nabywania, sprzedaży, dostarczania, rozpowszechniania lub udostępniania dla siebie lub innych haseł lub kodów zabezpieczających umożliwiające dostęp do danych (art. 202a ust. 2), lub oprogramowania do celu popełnienia takiego przestępstwa podlega karze pozbawienia wolności nieprzekraczającej jednego roku lub grzywnie". Zgodnie z art. 202c niemieckiego k.k. za niewłaściwe wykorzystanie urządzeń uważa się akty przygotowujące do szpiegostwa i wyłudzania informacji (tzw. *phishingu danych*).

Zgodnie z art. 303a k.k.[868] czyn polegający na manipulowaniu danymi jest karalny. Manipulowanie danymi polega na bezprawnym usuwaniu, tłumieniu, czynieniu danych bezużytecznymi lub

zmienianiu danych taki sposób, że tracą one na wartości. Taka osoba podlega karze pozbawienia wolności nieprzekraczającej dwóch lat lub grzywnie. Brak skutku w postaci wyrządzenia szkody przy wypełnieniu przez sprawcę pozostałych znamion występku z 303a k.k. jest równoznaczny z tym, że powinien on odpowiadać za usiłowanie tego przestępstwa.

Ingerencja w system to przestępstwo stypizowane w art. 303b k.k., tzw. sabotaż komputerowy. Natomiast każdy, kto zakłóca operacje przetwarzania danych, które mają istotne znaczenie dla innych, poprzez popełnienie przestępstwa na mocy art. 303a, wprowadzanie lub przesyłanie danych (art. 202a) z zamiarem spowodowania szkody innej osobie, umyślnego, bezprawnego poważnego zakłócania funkcjonowania systemu informatycznego przez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych, podlega karze pozbawienia wolności nieprzekraczającej trzech lat lub grzywnie. Jeżeli operacja przetwarzania danych ma istotne znaczenie dla działalności innej firmy, przedsiębiorstwa lub władzy publicznej, sprawca podlega karze pozbawienia wolności nieprzekraczającej pięciu lat lub grzywnie. Usiłowanie jest również karalną postacią zjawiskową przestępstwa.

W szczególnie poważnych przypadkach, o których mowa w ust. 2, kara wynosi od sześciu miesięcy do dziesięciu lat. Szczególnie poważny przypadek zazwyczaj występuje, jeśli sprawca powoduje poważne straty finansowe, działa na zasadach handlowych lub jako członek bandy, której celem jest nieprzerwane dokonywanie sabotażu komputerowego, przez przestępstwo zagraża zaopatrzeniu ludności w istotne towary lub usługi albo bezpieczeństwu narodowemu Republiki Federalnej Niemiec.

Fałszerstwo komputerowe w RFN zostało stypizowane w art. 267 k.k. Każdy, kto dopuszcza się fałszerstwa na zasadach komercyjnych jako członek gangu, którego celem jest ciągłe popełnianie przestępstw na mocy art. 263–240 lub art. 267–269, podlega karze pozbawienia wolności od jednego do dziesięciu lat, w mniej poważnych przypadkach pozbawienia wolności od sześciu miesięcy do pięciu lat. Zgodnie z art. 269 k.k. w sprawie fałszowania danych mających na celu

dostarczenie dowodu, każdy kto, dla celów oszustwa w legalnym obrocie handlowym przechowuje lub modyfikuje dane przeznaczone do dostarczenia dowodu w taki sposób, że fałszywy lub sfałszowany dokument zostałby stworzony po ich odzyskaniu lub wykorzystuje dane przechowywane bądź modyfikowane w taki sposób, podlega karze pozbawienia wolności nieprzekraczającej pięciu lat lub grzywnie.

Istotą przestępstwa określonego w art. 269 k.k. jest karalne fałszowanie dokumentu lub używanie sfałszowanego dokumentu jako autentycznego[869]. Celem ochrony jest zapewnienie zaufania do instytucji dokumentu, dlatego ustawodawca za karalne zachowania uznał zarówno jego podrabianie i przerabianie, jak i posługiwanie się tak sfałszowanym dokumentem, tj. zapewnienie ochrony przed fizycznym zamachem na jego autentyczność. Przedmiotem ochrony jest wiarygodność instytucji dokumentu w celu zapewnienia ochrony obrotowi prawnemu i gospodarczemu[870]. Indywidualnym przedmiotem ochrony są interesy (dobra) konkretnego pokrzywdzonego, określone przez rodzaj i treść prawa, wyrażonego w dokumencie stanowiącym przedmiot określonego przestępstwa. Dobrem tym może być np. informacja, mienie, a nawet życie lub zdrowie[871]. Czyn zabroniony można popełnić na trzy sposoby, tj. podrabiając albo przerabiając dokument, używając tak sfałszowanego dokumentu, z tym, że dla karalności tego czynu nie jest istotne, czy taki dokument zawiera prawdziwe, czy fałszywe informacje[872]. Czyn zabroniony w zakresie fałszerstwa (podrabianie lub przerabianie) może popełnić każdy, ale wyłącznie z zamiarem bezpośrednim – kierunkowym, natomiast w zakresie używania sfałszowanego dokumentu jako autentycznego można popełnić umyślnie, z zamiarem bezpośrednim albo ewentualnym.

Zgodnie z art. 267 ust. 3 i 4 niemieckiego kodeksu karnego stosuje się *mutatis mutandis*. Artykuł 263 k.k. oraz art. 263a k.k. regulują przestępstwo tzw. oszustwa komputerowego, a w szczególnie poważnych przypadkach karą jest pozbawienie wolności od sześciu miesięcy do dziesięciu lat. Szczególnie poważny przypadek występuje zazwyczaj, jeśli sprawca działa na zasadach handlowych lub jako członek bandy, której celem jest ciągłe popełnianie fałszerstw lub

oszustw, powoduje poważną stratę finansową lub działa w celu umieszczenia dużej liczby osób zagrożonych stratą finansową przez ciągłe popełnianie przestępstw związanych z oszustwami, umieszcza inną osobę w trudnej sytuacji finansowej, nadużywa swoich uprawnień lub stanowiska jako urzędnika publicznego lub udaje, że zdarzenie objęte ubezpieczeniem nastąpiło po tym, jak on lub inna osoba w tym celu podpalił przedmiot o znacznej wartości lub zniszczył go, w całości lub w części, przez podpalenie go lub spowodował zatonięcie lub zboczenie statku na brzeg.

Sekcja 184b niemieckiego kodeksu karnego obejmuje dystrybucję, nabywanie i posiadanie pornografii dziecięcej (1). Ktokolwiek: rozpowszechnia pornografię dziecięcą lub udostępnia ją ogółowi społeczeństwa – przy czym pornograficzne materiały pisemne (sekcja 11 [3]) są uważane za pornografię dziecięcą, jeśli dotyczą czynności seksualnych wykonywanych przez lub w obecności osoby poniżej czternastego roku życia (dziecko), reprodukcji dziecka w stanie pełnego lub częściowego rozebrania się w pozycji nienaturalnie wykazującej cechy płciowe, lubieżnego pokazywania niezamkniętych narządów płciowych lub nieosłoniętych pośladków dziecka, zobowiązuje się do posiadania innego rodzaju pornografii dziecięcej odtwarzającej rzeczywistą lub realistyczną działalność, wytwarza pornografię dziecięcą odtwarzającą rzeczywistą działalność lub produkuje, pozyskuje, dostarcza oferty, pochwala lub zobowiązuje się do importowania bądź eksportowania pornografii dziecięcej w celu korzystania z takiej pornografii dziecięcej lub kopii wykonanych z takich materiałów w rozumieniu nr 1 lub 2 powyżej lub sekcji 184d (1), lub w celu ułatwienia takiego wykorzystania, podlega karze pozbawienia wolności od trzech miesięcy do pięciu lat.

W przypadkach, o których mowa w ust. 1, karą będzie pozbawienie wolności od sześciu miesięcy do dziesięciu lat, jeżeli sprawca działa na zasadach komercyjnych lub jako członek bandy, której celem jest ciągłe popełnianie takich przestępstw, oraz w przypadkach podsekcji (1) o nr 1, 2 i 4 (3). Każdy, kto podejmie się posiadania pornografii dziecięcej, reprodukując rzeczywistą lub realistyczną działalność, lub ktokolwiek posiada taki materiał, podlega karze pozbawienia wolności nieprzekraczającej trzech lat lub grzywnie. Karze podlega również

próba. Nie dotyczy to przestępstw na podstawie podsekcji (1) o nr 2 i 4, a także przestępstw określonych w ust. (3). Podsekcja (1) nr 2 i ppkt (3) nie mają zastosowania do czynności, które służą wyłącznie spełnieniu następujących warunków: funkcje stanu, zadania wynikające z umów zawartych z kompetentną agencją rządową lub obowiązki służbowe albo zawodowe.

W przypadkach, o których mowa w ust. 2, zastosowanie ma sekcja 73d. Przedmioty, do których odnosi się przestępstwo, o którym mowa w ust. 1, 2, 3 lub ust. 3, podlegają zarządzeniu o pozbawieniu wolności. Zastosowanie ma sekcja 74a. Przestępstwa związane z pornografią dziecięcą zostały stypizowane w art. 184b i c k.k.

Niemiecki kodeks karny przewiduje również odpowiedzialność karną za podżeganie, usiłowanie i pomocnictwo (art. 23, 26 i 27 k.k.). Odpowiedzialność osób prawnych jest przewidziana w drodze ustawy o odpowiedzialności pomiotów prawnych (dotyczy kar nakładanych przedsiębiorstwa posiadające osobowość prawną i stowarzyszenia)[873].

6.3.2. INSTYTUCJONALNY WYMIAR POLITYKI CYBERBEZPIECZEŃSTWA RFN

Głównym organem federalnym w zakresie cyberbezpieczeństwa jest Federalny Urząd Bezpieczeństwa Teleinformatycznego (Bundesamt für Sicherheit in der Informationstechnik – BSI)[874], który podlega Ministerstwu Spraw Wewnętrznych. Urząd powstał w 1991 r., a siedzibę ma w Bonn. Pełni nadrzędną funkcję koordynacyjną i wyznaczającą główne kierunki działań w obszarze cyberbezpieczeństwa, w tym ochrony infrastruktury krytycznej, bezpieczeństwa internetowego, kryptografii oraz certyfikacji i akredytacji produktów i audytorów bezpieczeństwa IT.

Ustawa o bezpieczeństwie IT zawiera wiele postanowień wzmacniających rolę BSI jako centralnego punktu gromadzącego i analizującego informacje w zakresie cyberbezpieczeństwa. Głównym zadaniem urzędu jest ocena raportów dotyczących potencjalnych cyberataków na infrastrukturę krytyczną. Urząd współpracuje m.in. z Federalną Służbą Wywiadu i Federalnym Urzędem Ochrony Konstytucji (jest to służba kontrwywiadowcza), a także z innymi

organami w ramach Narodowego Centrum Przeciwdziałania Cyberzagrożeniom.

W § 3 ustawy BSI został wyposażony w następujące kompetencje:

- wydawanie ostrzeżeń;
- wydawanie zaleceń odnośnie do środków bezpieczeństwa lub wykorzystania określonych produktów bezpieczeństwa;
- prawo do kontroli produktów i systemów IT;
- opracowanie minimalnych standardów cyberbezpieczeństwa dla infrastruktury federalnej, które zostaną przyjęte w formie aktów wykonawczych do ustawy o bezpieczeństwie IT.

BSI odgrywa także istotną rolę informacyjną. W 2016 r. wydało raport o stanie bezpieczeństwa IT w Niemczech (*Die Lage der IT-Sicherheit in Deutschland 2016*)[875]. Zawiera on kompleksowy przegląd techniczny słabych punktów systemu i aktualnych zagrożeń. Utworzenie wielu organów państwowych posiadających kompetencje w obszarze cyberbezpieczeństwa przewidziała *Strategia* z 2011 r. Postulowano w niej powołanie Narodowego Centrum Przeciwdziałania Cyberzagrożeniom (Nationales Cyber-Abwehrzentrum – NCAZ) oraz Narodowej Rady Cyberbezpieczeństwa (Nationaler Cyber-Sicherheitsrat). Raport o stanie bezpieczeństwa IT w Niemczech opisuje i analizuje aktualną sytuację w zakresie bezpieczeństwa IT, przyczyny ataków cybernetycznych oraz środki i metody wykorzystywane w ataku[876].

Rozwiązania przewidziane w dyrektywie 2016/1148/UE zostały wprowadzone w niemieckim porządku prawnym ustawą z dnia 25 lipca 2015 r. o zmianie ustawy z dnia 14 sierpnia 2009 r. o Federalnym Urzędzie ds. Bezpieczeństwa Informacji (BSI). Ustawa zmienia istniejące ustawy o bezpieczeństwie infrastruktury krytycznej, prawie telekomunikacyjnym i inne, nie tworząc jednak w pełni spójnego systemu. Nałożyła na różne podmioty (przede wszystkim operatorów infrastruktury krytycznej i przedsiębiorców telekomunikacyjnych) nowe obowiązki dotyczące stosowania odpowiednich środków bezpieczeństwa, informowania klientów czy organów władzy publicznej o możliwych nadużyciach czy zagrożeniach. BSI dostał dodatkowe kompetencje w zakresie opracowywania standardów

dotyczących cyberbezpieczeństwa, kontaktów z organami właściwymi. Do jego zadań należy bieżąca analiza zagrożeń, przygotowywanie środków do ich zwalczania oraz zabezpieczanie przed nimi gospodarki.

BSI pełni funkcję federalnego urzędu ds. cyberbezpieczeństwa. Do jego zadań należy bieżąca analiza zagrożeń, przygotowywanie środków do ich zwalczania oraz zabezpieczanie przed nimi gospodarki. W jego ramach funkcjonuje *Cyber-Abwehrzentrum* (Cyber-AZ), którego zadaniem jest koordynacja ochrony cyberprzestrzeni w Niemczech przez wczesne ostrzeganie, informację i prewencję. BSI zatrudnia ok. 600 pracowników, a Cyber-AZ – 10 pracowników delegowanych.

W stosowanie prawa dotyczącego bezpieczeństwa teleinformatycznego ponadto są zaangażowane Federalne Ministerstwo Spraw Wewnętrznych, Federalny Urząd Ochrony Ludności i Pomocy w przypadku katastrof, państwa związkowe (landy), departamenty federalnych ministerstw: Transportu i Infrastruktury Cyfrowej, Gospodarki i Technologii, Edukacji i Nauki. Liczba operatorów usług kluczowych w Niemczech obejmuje ok. 1885 podmiotów, które są objęte dwoma pakietami rozporządzeń. W Niemczech ustawa wprowadziła sektor spożywczy niewystępujący w załączniku 2 dyrektywy 2016/1148/UE dyrektywy, nie objęła natomiast administracji publicznej z uwagi na federalną strukturę państwa.

Narodowe Centrum Przeciwdziałania Cyberzagrożeniom z siedzibą w Bonn jest platformą umożliwiającą współpracę organów niemieckiej administracji właściwych w sprawach ochrony cyberprzestrzeni. Organ rozpoczął działalność w kwietniu 2011 r. i według założeń ma być pierwszym ogniwem walki z zagrożeniami cybernetycznymi. Pracami zarządza Federalny Urząd Bezpieczeństwa Teleinformatycznego (BSI) i to w jego strukturach działa Centrum. Do najważniejszych zadań Centrum należą przeciwdziałanie zagrożeniom w cyberprzestrzeni oraz ich zwalczanie, w tym wymiana informacji, analiza incydentów teleinformatycznych i ich ewaluacja, wypracowywanie mechanizmów skutecznej ochrony i prewencji oraz neutralizacja rezultatów ataków, a także ocena skuteczności realizacji

postanowień strategii ochrony cyberprzestrzeni. Zrzeszone w Centrum organy dostarczają informacji zgodnie z właściwością rzeczową, a BSI ocenia incydent pod względem technicznym. W działalność NCAZ zaangażowanych jest wiele jednostek policyjnych i służb specjalnych: Federalny Urząd Ochrony Konstytucji (Bundesamt für Verfassungsschutz – BfVSchG)[877], Federalny Urząd Ochrony Ludności i Reagowania Kryzysowego (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – BBK)[878], Federalny Urząd Kryminalny (Bundeskriminalamt – BKA)[879], Federalna Służba Wywiadu (*Bundesnachrichtendienst* – BND)[880], Celny Urząd Kryminalny (Zollkriminalamt – ZKA)[881] oraz policja federalna (Bundespolizei – BPol)[882]. Do prac NCAZ została oddelegowana także Bundeswehra.

BfVSchG bada, czy za atak odpowiada zagraniczna służba specjalna, a BBK ocenia skutki zamachów dla infrastruktury krytycznej. Pozostałe organy rozpoznają nowe metody i narzędzia ataku. W konsekwencji NCAZ potrafi w krótkim czasie przedstawić aktualną i kompleksową informację na temat zagrożeń dla cyberprzestrzeni. W ramach działań prewencyjnych NCAZ okresowo, a dodatkowo również w razie potrzeby przedstawia Narodowej Radzie Cyberbezpieczeństwa stosowne wytyczne, w sytuacjach nadzwyczajnych raportuje bezpośrednio sztabowi kryzysowemu w MSW[883].

Przedmiotem zmian legislacyjnych w wymienionych aktach prawnych jest to, że agencjom ochrony takim jak Federalny Urząd Ochrony Konstytucji, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Federalnego czy Celny Urząd Kryminalny i Federalny Urząd Policji Kryminalnej zapewniono niezbędne kompetencje dochodzeniowo-śledcze w tym zakresie, włącznie z cyberprzestępczością. Mogą one także pozyskiwać stosowne informacje od władz migracyjnych. Dopiero gdy wszystkie niemieckie władze zostały w pełni zaangażowane w działania antyterrorystyczne, można uznać, że wejście w życie tej ustawy jest w stanie zapobiec terroryzmowi i zarazem daje możliwość stosowania zaostrzonej polityki migracyjnej podyktowanej względami bezpieczeństwa państwa[884].

Federalny Urząd Ochrony Konstytucji może stosować w warunkach określonych w § 8 ust. 2 zd. 1 środki techniczne w celu określania

położenia terminali mobilnych lub aktywnie podłączonych do określonego urządzenia lub w celu ustalenia numeru karty. Środek jest dozwolony tylko w przypadku braku możliwości zastosowania innych środków technicznych wymienionych w zd. 1 w celu identyfikacji terminali na miejscu albo w celu ustalenia liczby urządzeń lub gdy ustalenie numeru karty jest o wiele bardziej trudne. Dane osobowe osób trzecich mogą być pobierane przy okazji takiego działania, jeśli jest to nieuniknione ze względów technicznych, w celu osiągnięcia celu określonego w zd. 1. Takie osoby można skazać tylko na podstawie § 8a ust. 3 nr 1 i 2 pkt b.[885]

Zmiany w ustawie o Federalnym Urzędzie Policji Kryminalnej rozszerzyły zakres jej kompetencji śledczych w celu uwzględnienia niektórych poważnych typów przestępstw, a także wzmocniły uprawnienia Federalnego Urzędu Policji Kryminalnej zarówno jako centrali administracji, jak i federalnego państwa związkowego przez rozszerzenie jego uprawnienia na pozyskiwanie danych. Regulacje odnoszące się do prawa o cudzoziemcach miały na celu:

- przyznanie organom bezpieczeństwa koniecznych prawnych kompetencji;
- wzmocnienie koniecznej wymiany danych między władzami;
- zapobieganie przestępcom terrorystycznym przyjeżdżającym do Niemiec;
- poprawę środków w celu zapewnienia bezpieczeństwa tożsamości podczas procedury wizowej;
- umożliwienie tzw. powietrznym szeryfom (zbrojnym członkom Federalnej Straży Granicznej) wykorzystywania niemieckich statków powietrznych do zapewnienia i przywrócenia bezpieczeństwa oraz ochrony na pokładzie samolotu;
- zwiększenie środków do przeprowadzenia lepszej kontroli granicy;
- zidentyfikowanie ekstremistów, którzy są obecni na terytorium Niemiec[886].

Według założeń ustawy z 20 grudnia 1990 r. Federalna Służba Wywiadowcza jest organem federalnym pod jurysdykcją Urzędu

Kanclerskiego. Dlatego departament policji nie może być związany z Federalną Służbą Wywiadowczą, której zadaniem jest:

- gromadzenie i zbieranie informacji o obcych państwach;
- wykorzystywanie informacji na temat zagranicznych państw, których polityka bezpieczeństwa może powodować implikacje polityczne dla Republiki Federalnej Niemiec;
- przetwarzanie niezbędnych informacji.

W myśl § 2 ustawy BNDG posiada następujące kompetencje:

- ma prawo chronić swoich ludzi, miejsca, przedmioty i środki, aby wpłynąć na bezpieczeństwo państwa;
- może podejmować działania niezbędne do kontroli bezpieczeństwa osób, które pracują dla BNDG;
- ma prawo weryfikacji wykonywanych zadań oraz dostępu do niezbędnych informacji;
- jest odpowiedzialna za dostęp innych organów władzy do wydarzeń za granicą, które mają wpływ na polityczne bezpieczeństwo RFN.

Narodowa Rada Cyberbezpieczeństwa została powołana 23 lutego 2011 r. Jest organem koordynującym współpracę między organami administracji, a także z prywatnymi podmiotami, w tym głównie przedsiębiorcami. Na jej czele stoi pełnomocnik rządu ds. teleinformatycznych. W skład Rady wchodzą przedstawiciele Urzędu Kanclerskiego, Ministerstwa Obrony, Ministerstwa Spraw Zagranicznych, Ministerstwa Spraw Wewnętrznych, Ministerstwa Gospodarki i Energii, Ministerstwa Sprawiedliwości i Ochrony Konsumenta oraz Ministerstwa Finansów, a także państw związkowych (landów) oraz tzw. stowarzyszonych członków – prywatnych partnerów będących przedstawicielami niemieckiej gospodarki. Celem Rady jest przede wszystkim analiza dostępnych instrumentów prewencji oraz zadań politycznych przez przedstawicieli państwa i gospodarki. Organ spotyka się trzy razy w roku[887]. W razie potrzeby ten skład jest poszerzany o dalsze resorty, przedstawicieli biznesu i świata nauki. Przedmiotowemu organowi powierzono koordynację współpracy w obrębie niemieckiego rządu, a także na styku państwa i gospodarki.

Mimo że w Niemczech kompetencje z zakresu cyberbezpieczeństwa należą przede wszystkim do jednostek cywilnych, posiada je również Bundeswehra. Od 1 stycznia 2013 r. działa Centrum Operacyjne Systemów IT Bundeswehry (Betriebszentrum IT-System der Bundeswehr – BITS) z siedzibą w Rheinbach[888]. Jest to autonomiczna jednostka w ramach armii. W Centrum zatrudnionych jest ok. 600 żołnierzy i 80 pracowników cywilnych, którzy zostali podzieleni na cztery wydziały: zarządzania ryzykiem i bezpieczeństwem IT, zarządzania IT, planowania, zarządzania i realizacji oraz operacyjny.

Główne zadanie Centrum Operacyjnego sprowadza się do ochrony systemów IT należących do Bundeswehry – nie tylko lokalnie, ale również np. na zagranicznych misjach i operacjach. W ramach tego nadrzędnego zadania jednostka może m.in. przeprowadzać ćwiczenia wewnątrz kraju i poza jego granicami.

Ważnym organem jest także Zespół Reagowania na Incydenty Komputerowe Bundeswehry (Computer Emergency Response Team der Bundeswehr – CERTB), który rozpoczął działalność w 2002 r. w Euskirchen. Jego zadaniem jest monitorowanie, utrzymywanie i ewentualne przywracanie sprawności systemom IT Bundeswehry. Zespół zatrudnia ok. 60 specjalistów[889].

Należy również wspomnieć o jednostce badawczej, jaką jest Centrum Badań Cyberobrony (CODE), które działa w ramach Uniwersytetu Bundeswehry w Monachium[890]. Zadania tego organu skupiają się na przeciwdziałaniu i zwalczaniu zagrożeń w cyberprzestrzeni przez wymianę informacji, ocenę incydentów, opracowywanie mechanizmów ochrony i prewencji, usuwanie skutków ataków oraz analizę skuteczności strategii cyberbezpieczeństwa. Okresowo przedstawia wytyczne Narodowej Radzie Cyberbezpieczeństwa. W sytuacjach nadzwyczajnych Centrum podlega bezpośrednio sztabowi kryzysowemu w Ministerstwie Spraw Wewnętrznych.

6.4
IMPLEMENTACJA POLITYKI

CYBERBEZPIECZEŃSTWA WE FRANCJI

6.4.1. PODSTAWOWE DOKUMENTY W ZAKRESIE POLITYKI CYBERBEZPIECZEŃSTWA

Francuska strategia cyberbezpieczeństwa, czyli tzw. *Biała Księga* z 2008 r., określiła zagrożenia związane z atakami informatycznymi wymierzonymi w najważniejsze elementy infrastruktury państwa jako jedne z najbardziej prawdopodobnych zagrożeń w kolejnych 15 latach. Wskazała równocześnie na wiążące się z tego rodzaju zdarzeniem poważne skutki dla funkcjonowania społeczeństwa i wszystkich aspektów życia publicznego. Dokument określał instrumenty informatyczne i komunikacyjne jako system nerwowy społeczeństwa, bez którego jego prawidłowe funkcjonowanie byłoby niemożliwe. *Biała Księga* była pierwszym oficjalnym dokumentem, w którym zagrożenia w cyberprzestrzeni określono mianem poważnych. Jako ich potencjalne formy wymieniono m.in. działalność polegającą na atakach hakerskich czy zorganizowaną przestępczość[891].

Główne tezy *Białej Księgi* sprowadzają się do stwierdzenia, że państwo powinno wypracować instrumenty pozwalające na skuteczne zwalczanie zagrożeń w cyberprzestrzeni – cel ten powinien stać się jednym z priorytetów Francji w sferze bezpieczeństwa narodowego. W dokumencie podkreślono konieczność wypracowania zdolności wczesnego wykrywania ataków informatycznych i reagowania na incydenty mające zarówno charakter ściśle ukierunkowany na określone sieci czy urządzenia, jak i na działania o charakterze masowym. W sferze zapobiegania zagrożeniom zaproponowano wykorzystywanie urządzeń i sieci mających wysoki stopień zabezpieczeń i stworzenie katalogu kompetencji oraz instrumentów, którymi w razie zagrożenia mogłyby się posługiwać organy administracji publicznej i tzw. operatorzy infrastruktury krytycznej[892]. Efektem tego było przyjęcie dekretu nr 2008-934 z 7 lipca 2009 r.[893]

Francuska definicja cyberprzestrzeni wywodząca się ze strategii cyberbezpieczeństwa została zawarta w dokumencie przygotowanym w 2011 r. przez francuską Krajową Agencję Bezpieczeństwa Systemów

Informacyjnych (ANSSI) *Obrona oraz bezpieczeństwo systemów informacyjnych. Strategia dla Francji*[894]. Sformułowana tam definicja lakonicznie określiła cyberprzestrzeń jako „przestrzeń komunikacyjną utworzoną przez globalne połączenie sprzętu służącego do automatycznego przetwarzania danych cyfrowych [895]". Definicja francuska nie porusza bezpośrednio kwestii dotyczących użytkowników ni szerszego spektrum zjawisk społecznych czy ekonomicznych, skupiając się w całości na określeniu cyberprzestrzeni jako przestrzeni komunikacyjnej opierającej się na infrastrukturze rozsianej na całym świecie. Taka definicja może prowadzić do wniosku, że cyberprzestrzeń wydaje się bardziej obszerna niż Internet[896].

Oprócz przytoczonej definicji francuska strategia cyberbezpieczeństwa dostarcza innych, ciekawych wniosków na temat cyberprzestrzeni nieujętych wprost w definicji. Cyberprzestrzeń nie tylko zbliża, ale wręcz powoduje mieszanie się kultur, gromadząc idee oraz informacje pochodzące z całego świata.

Ponadto w strategii z 2011 r. wymieniono cztery cele strategiczne, do których osiągnięcia Francja ma zmierzać przez działania podejmowane w sferze cyberbezpieczeństwa. Są to:

- uzyskanie statusu mocarstwa w sferze cyberobrony;
- zagwarantowanie autonomii decyzyjnej przez ochronę informacji istotnych z punktu widzenia suwerenności Francji;
- poprawa cyberbezpieczeństwa najważniejszych elementów infrastruktury krytycznej;
- zapewnienie bezpieczeństwa w cyberprzestrzeni.

Zgodnie z tymi założeniami Francja powinna się stać jednym z najbardziej rozwiniętych w sferze cyberobrony państw UE, zachowując jednocześnie wysoki stopień autonomii w wymiarze strategicznym. W dokumencie zwraca się uwagę na ścisły związek między tymi dwiema kompetencjami a pozycją państwa na arenie międzynarodowej. Skuteczna ochrona sieci informatycznych jest niezbędna z uwagi na intensyfikację działań wywiadowczych prowadzonych przez inne państwa, których celem jest uzyskanie dostępu do informacji istotnych dla zachowania suwerenności państwa. Cel drugi był ściśle

powiązany z dwoma aspektami istotnymi dla systemu cyberbezpieczeństwa: ogólnymi celami polityki kontrwywiadowczej państwa oraz rozwojem zdolności technologicznych w zakresie bezpieczeństwa informacji[897]. Najbardziej efektywnym środkiem zapobiegania nieuprawnionemu uzyskaniu dostępu do tego rodzaju informacji jest stosowanie technik kryptograficznych uniemożliwiających lub opóźniających uzyskanie do nich faktycznego dostępu lub zrozumienie ich treści. Trzeci cel wiąże się z tym, że rosnące współzależności między sferami gospodarki i informatyki sprawiają, że bezpieczeństwo sieci informatycznych jest jednym z podstawowych warunków utrzymania rozwoju gospodarczego na odpowiednim poziomie. W razie poważnego zakłócenia funkcjonowania sieci telekomunikacyjnych czy Internetu wypracowanie alternatywnych metod wymiany informacji okazałoby się utrudnione lub niemożliwe, biorąc pod uwagę stale zwiększający się stopień informatyzacji we wszystkich obszarach gospodarki i przemysłu. Z tego powodu rozwój nowoczesnych metod reagowania na zagrożenia w cyberprzestrzeni jest jednym z narodowych priorytetów Francji. Cel czwarty jest powiązany z potencjalnymi zagrożeniami takimi jak kradzież tożsamości, haseł do kont bankowych oraz handel bazami zawierającymi dane osobowe. Coraz częstszym zjawiskiem jest też zdalne przejmowanie kontroli nad urządzeniami informatycznymi przez tzw. botnety. Zadaniem właściwych organów państwa jest zatem zapewnienie odpowiedniego poziomu zaufania do usług świadczonych drogą elektroniczną oraz innych powszechnie wykorzystywanych instrumentów informatycznych.

Narodowa doktryna ochrony cyberprzestrzeni z 2013 r.[898] jest oparta na komplementarnych i całościowych działaniach, których podstawą są:

- wypracowanie wydajnych i odpornych na ataki cybernetyczne mechanizmów ochrony systemów informatycznych organów państwowych, operatorów infrastruktury krytycznej oraz strategicznie istotnych przedsiębiorstw, które są połączone z operacyjną organizacją działań obronnych. Elementy te mają być koordynowane przez premiera, a wszelkie działania mają być

oparte na ścisłej współpracy poszczególnych organów w celu jak najszybszego wykrywania zagrożeń;
- stworzenie całościowych i dostosowanych do okoliczności zróżnicowanych mechanizmów reagowania działających na zasadzie subsydiarności, które polegają na wykorzystaniu w pierwszej kolejności środków prawnych, dyplomatycznych oraz policyjnych, dopuszczających jednakże możliwość stopniowego stosowania mechanizmów znajdujących się w kompetencji Ministerstwa Obrony, jeżeli będą zagrożone strategiczne interesy państwa.

Odpowiedzią na ogłoszoną doktrynę było stworzenie tzw. *Paktu cyberobrony*[899], który zwraca uwagę na konieczność wypracowania skutecznych mechanizmów ochrony przed atakami cybernetycznymi z uwagi na postępującą informatyzację poszczególnych komponentów sił zbrojnych. Podmioty te wykorzystują zaawansowane i najistotniejsze – pod kątem strategicznym – systemy informatyczne związane m.in. z zarządzaniem instrumentami odstraszania nuklearnego czy zaawansowanymi systemami obronnymi wykorzystywanymi przez wojska lądowe, powietrzne i marynarkę wojenną. W konsekwencji bezpieczeństwo cybernetyczne jest jednym z priorytetowych obszarów działań Ministerstwa Obrony[900].

Pakt cyberobrony określał wszystkie działania, które miały zostać zrealizowane w latach 2014–2016 zgodnie z ustawą o programowaniu wojskowym na lata 2014–2019. Dotyczyły one:
- podniesienia poziomu bezpieczeństwa systemów informatycznych oraz wzmocnienia instrumentów ochrony i reagowania wykorzystywanych przez Ministerstwo Obrony i jego najważniejszych partnerów;
- intensyfikacji działań w sferze badań i rozwoju;
- właściwego wykorzystania potencjału ludzkiego oraz stworzenia spójnego systemu kształcenia i zatrudnienia wyspecjalizowanych kadr;
- rozwoju centrum eksperckiego cyberobrony w Bretanii;
- rozwoju współpracy z partnerami zagranicznymi;
- wspierania procesu tworzenia narodowej wspólnoty cyberobrony.

Kolejna francuska *Strategia Narodowa Bezpieczeństwa Cybernetycznego* została ogłoszona przez premiera Francji Manuela Vallsa 16 października 2015 r. Strategia miała na celu poprawę przepływu danych w cyberprzestrzeni oraz ich skuteczniejszą ochronę. Francja dążyła również do autonomicznej działalności cyfrowej[901]. Polityka ochrony cyberprzestrzeni jest definiowana jako „zachowanie zdolności do podejmowania decyzji na podstawie wiarygodnych informacji oraz zabezpieczenia integralności francuskich systemów obronnych". Ponadto w tym dokumencie wymieniono pięć celów strategicznych, do których osiągnięcia Francja ma zmierzać przez działania podejmowane w sferze cyberbezpieczeństwa. Są to:

- obrona i bezpieczeństwo państwowych systemów informacyjnych oraz infrastruktury krytycznej przed poważnym kryzysem cyberbezpieczeństwa;
- stworzenie cyfrowego zaufania, ochrona prywatności i danych osobowych przed cyberprzestępczością;
- podnoszenie świadomości zagrożenia w sieci, szkolenia, kontynuacja edukacji na różnych poziomach;
- internacjonalizacja francuskiego środowiska biznesu i technologii cyfrowych;
- osiągnięcie cyfrowej autonomii strategicznej w cyberprzestrzenie europejskiej.

Zgodnie z jej koncepcją zadaniem państwa w cyberprzestrzeni jest zapewnienie wolności wypowiedzi i działania we Francji, a także bezpieczeństwa infrastruktury krytycznej w przypadku poważnych cyberataków (cel 1), by chronić cyfrowe życie obywateli i przedsiębiorstw oraz zwalczać cyberprzestępczość (cel 2), aby zapewnić wymaganą edukację i szkolenia dla bezpieczeństwa cyfrowego (cel 3), potrzebnych do wniesienia wkładu w rozwój środowiska, któremu sprzyja zaufanie do technologii cyfrowej (cel 4) i promowanie współpracy między państwami członkowskimi UE Unii (UE) w sposób sprzyjający powstaniu europejskiej cyfrowej autonomii strategicznej, w perspektywie długoterminowej jako gwaranta

cyberprzestrzeni, która jest bardziej bezpieczna i pełna szacunku dla wspólnych wartości (cel 5).

Cel pierwszy zakłada rozwijanie autonomicznego myślenia strategicznego, wspieranego dzięki światowej wiedzy technicznej Francji. Ma to zapewnić stałą obronę jej podstawowych interesów w cyberprzestrzeni. Równolegle Francja będzie kontynuować wzmocnienie bezpieczeństwa jego krytycznych sieci i odporność w przypadku poważnego cyberataku, rozszerzając współpracę z prywatnymi interesariuszami na szczeblach krajowym i międzynarodowym.

Cel drugi zakłada, że cyberprzestrzeń pozostanie bezpieczna dla wszystkich firm i obywateli. Zostanie to zapewnione przez środki ochronne i działania naprawcze, które będą dotyczyły wykorzystania danych osobowych, oraz opracowanie cyfrowych produktów zabezpieczających dostosowanych do potrzeb publicznych. Działania naprawcze zostaną przeprowadzone wobec ofiar cyberprzestępczości, zapewniając im techniczną i prawną pomoc.

Cel trzeci jest ściśle związany z podnoszeniem poziomu edukacji uczniów i studentów, ponieważ jednostkom nadal brakuje wystarczającej świadomości o zagrożeniach związanych z cyfryzacją społeczeństwa. Aby sprostać rosnącym żądaniom ze strony sektorów publicznego i prywatnego dotyczącym cyberbezpieczeństwa, będą przeprowadzane szkolenia ekspertów w tej dziedzinie.

Cel czwarty jest powiązany ze wspólnym rozwojem rynków cyfrowych na całym świecie. Ma to stanowić możliwość zróżnicowania francuskich produktów cyfrowych i usług, które mają poziom bezpieczeństwa dostosowany do ich zastosowań. Wspierając inwestycje, innowacje i eksport w drodze zamówień publicznych, Francja stworzy sprzyjające środowisko dla francuskich firm oferujących bezpieczne produkty i usługi.

Cel piąty stał się poważnym wyzwaniem dla Francji wraz z podobnie myślącymi państwami członkowskimi UE, które również dążą do uzyskania statusu mocarstwa w sferze cyberobrony. Francja próbuje wzmocnić swój wpływ w organach międzynarodowych i zapewnić wsparcie najsłabiej chronionym państwom, aby budować swoje

możliwości w zakresie cyberbezpieczeństwa i przyczyniać się do ogólnej stabilności cyberprzestrzeni UE.

Warto zauważyć, że Francja już we wstępie określa cyberprzestrzeń jako „nową domenę nieuczciwej konkurencji i szpiegostwa, dezinformacji, propagandy, terroryzmu i przestępczości". Jest to bardzo nietypowa, aczkolwiek trafna definicja odnosząca się do stanu faktycznego, oparta na prawie karnym.

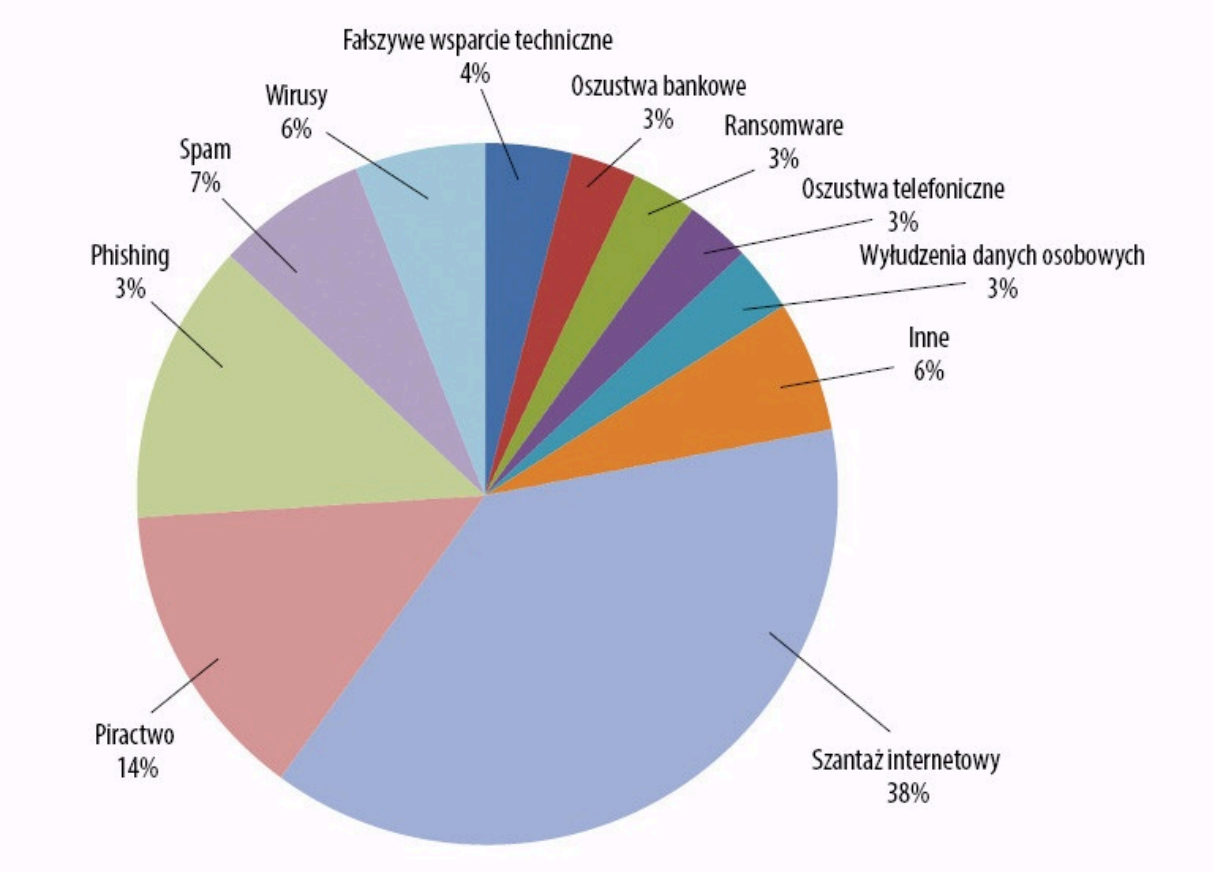
Republika Francuska jest jedynym państwem Unii Europejskiej, w którym celem polityki bezpieczeństwa cybernetycznego jest także rozwój zdolności o charakterze ofensywnym, pozwalających na wsparcie operacji wojskowych[902]. Założenie to powoduje, że podsystem militarny ochrony cybernetycznej funkcjonuje samodzielnie, a nadzór nad tymi przedsięwzięciami sprawuje minister obrony. W jego ramach prowadzone są działania o charakterze defensywnym w zasadzie ukierunkowanym na ochronę wojskowej infrastruktury informatycznej oraz ofensywnym. Ich zasadniczym celem jest zapewnienie tzw. suwerenności informacyjnej Francji. Zakres prowadzonych działań sprowadza się do zapewnienia ciągłości i niezakłóconej funkcjonalności militarnych oraz wykorzystywanych przez siły zbrojne sieci i systemów informatycznych.

Przyjęta w 2017 r. *Doctrine interarmées 3.40_Cyberdefence-3*[903] opiera się na technologiach i sprzęcie, które muszą być wydajne, solidne chronione w szczególności przed cyberzagrożeniami państwa, spełniające wymagania interoperacyjności między komponentami i sojusznikami oraz zgodne z ergonomią dostosowaną do środowiska operacyjnego i sprzyjające łatwości wdrożenia. Rozwój technologii i materiałów powinien natomiast mieć na celu poprawę wydajności operacyjnej ze szczególnym naciskiem na aspekty digitalizacji i łączności oraz na ergonomię, biorąc pod uwagę wymagania bezpieczeństwa sił i osób trzecich oraz ochronę przed zagrożeniami (zwłaszcza wysiłek w zakresie integralności danych i ochrony cybernetycznej).

Z kolei przepisy dotyczące bezpieczeństwa teleinformatycznego zostały wprowadzone do ustawy z dnia 18 grudnia 2013 r. o planowaniu wojskowym[904], która definiuje operatorów o istotnym znaczeniu, zbliżonych do definicji operatorów usług kluczowych

zapisanej w dyrektywie 2016/1148/UE. Ustawa przewiduje, że operatorzy o istotnym znaczeniu powinni przestrzegać konkretnych środków bezpieczeństwa teleinformatycznego i są zobowiązani do zgłaszania incydentów do ANSSI. Agencja zapewnia wsparcie tym operatorom, wydając wytyczne bezpieczeństwa teleinformatycznego. Jest zaangażowana w koordynację implementacji dyrektywy 2016/1148/UE. Francja w art. 15 ustawy o planowaniu wojskowym na lata 2014–2019 szczegółowo określa obowiązki, jakie prezes Rady Ministrów może nałożyć na operatorów o istotnym znaczeniu (OIV) w zakresie zabezpieczenia ich sieci, kwalifikacje ich systemów wykrywania, informacje o atakach, którym mogą być poddani, i poddaniu się kontrolom. Fakt, że obowiązki te zostały uregulowane w ustawie o programowaniu wojskowym, pokazuje, że obronność i bezpieczeństwo narodowe muszą być traktowane kompleksowo i spójnie. Artykuł 22 tej ustawy nakłada na OIV obowiązek wprowadzenia sprzętu do wykrywania ataków komputerowych i obsługi go przez usługodawców wykwalifikowanych przez ANSSI lub przez inne służby rządowe wyznaczone przez prezesa Rady Ministrów.

Aktualne podejście do implementacji NIS zakłada, że wymagania bezpieczeństwa dla operatorów usług kluczowych będą podobne jak dla operatorów infrastruktury krytycznej, a liczba operatorów usług kluczowych będzie większa niż liczba podmiotów objętych wymaganiami z zakresu infrastruktury krytycznej. Obecnie we Francji zidentyfikowano ponad 200 operatorów infrastruktury krytycznej w 12 sektorach. ANSSI będzie wyznaczone zarówno jako pojedynczy punkt kontaktowy, jak i organ właściwy w zakresie bezpieczeństwa sieci i informacji. Ustawa przewiduje również sankcje karne stosowane w przypadku nieprzestrzegania tych obowiązków.



RYSUNEK 6.10
Odsetek cyberprzestępstw we Francji w 2019 r. (stan na 9 lipca 2020 r.)

Źródło: Raport informacyjny senatu z dnia 9 lipca 2020 r. nr 613 opracowany przez M.S. Joissains i M. Jacques Bigot.

Francja wprowadziła wiele zmian do swojego ustawodawstwa, aby dostosować się do ewolucji cyberprzestępczości. Ustawa o zaufaniu do gospodarki cyfrowej z 2004 r.[905] zezwoliła w szczególności na ratyfikację *Budapeszteńskiej konwencji o cyberprzestępczości*, którą Francja ratyfikowała 10 stycznia 2006 r., czego efektem było wprowadzenie wymienionych w dalszej części zmian do kodeksu karnego[906] dotyczących np. regulacji takich przestępstw jak stalking, prześladowanie najbliższych, cyberszpiegostwo, rozpowszechnianie treści pornograficznych w sieci. Francja przyjęła także konwencję stambulską, konwencję z Lanzarote wraz z protokołem w sprawie ksenofobii i rasizmu.

Zgodnie z art. 222-33-2 k.k. stalking, fakt nękania innych przez powtarzające się komentarze lub zachowania, których celem lub skutkiem jest pogorszenie warunków pracy, które mogą naruszyć ich prawa i godność, zmienić ich zdrowie fizyczne lub psychiczne lub zagrozić ich przyszłości zawodowej, podlega karze dwóch lat pozbawienia wolności i grzywny w wysokości 30 tys. euro, gdy spowodowały całkowitą niezdolność do pracy dłuższą niż osiem dni, zostały popełnione na małoletnim w wieku piętnastu lat, zostały popełnione na osobie, której szczególna podatność ze względu na wiek, chorobę, ułomność, ułomność fizyczną lub psychiczną albo na stan ciąży, jest widoczna lub znana autorowi, zostały popełnione przy użyciu usługi komunikacji online dla społeczeństwa. Przestępstwo to podlega do karze trzech lat pozbawienia wolności i grzywnie w wysokości 45 tys. euro, jeżeli popełniono je w dwóch spośród okoliczności wcześniej wymienionych.

Zgodnie z art. 222-33-2-1 (prześladowanie najbliższych) prześladowanie współmałżonka, partnera związanego umową cywilną lub konkubenta przez powtarzające się uwagi lub zachowania, których przedmiotem lub skutkiem jest pogorszenie jego warunków życia skutkujące pogorszeniem jego zdrowia fizycznego lub psychicznego, podlega karze trzech lat pozbawienia wolności i grzywnie w wysokości 45 tys. euro. Jeżeli fakty te spowodowały całkowitą niezdolność do pracy krótszą lub równą ośmiu dniom lub nie skutkowały żadną niezdolnością do pracy, może być ukarany pięcioletnią karą pozbawienia wolności oraz grzywną w wysokości 75 tys. euro w przypadku całkowitej niezdolności do pracy przez ponad osiem dni. Te same kary nakłada się, gdy przestępstwo to popełnia były małżonek lub były partner pokrzywdzonego, lub były partner powiązany z tym ostatnim umową cywilną.

W myśl art. 222-33-2-2 uporczywy stalking to nękanie osoby przez powtarzające się uwagi lub zachowania, których przedmiotem lub skutkiem jest pogorszenie jej warunków życia skutkujące zmianą jej stanu zdrowia fizycznego lub psychicznego. Podlega on karze pozbawienia wolności do roku i grzywny 15 tys. euro, jeżeli te fakty spowodowały całkowitą niezdolność do pracy krótszą lub równą ośmiu dniom, lub nie spowodowały niezdolności do pracy.

Zgodnie z art. 222-13 dotyczącym prowokacji samobójczej doprowadzenie do samobójstwa innej osoby podlega karze trzech lat pozbawienia wolności i grzywnie w wysokości 45 tys. euro, jeśli po prowokacji nastąpiło samobójstwo lub próba samobójcza. Kary podwyższają się do pięciu lat pozbawienia wolności i grzywny w wysokości 75 tys. euro, jeżeli ofiarą przestępstwa jest nieletnia piętnastoletnia osoba. Osoby fizyczne lub prawne winne tego przestępstwa podlegają również karze dodatkowej: zakazu prowadzenia działalności przez podmiot prowadzący ustawiczne szkolenie zawodowe w rozumieniu przez okres pięciu lat.

W myśl art. 223-14 propaganda lub reklama, niezależnie od formy, na rzecz produktów, przedmiotów lub metod zalecanych jako środek zabójczy, podlega karze do trzech lat pozbawienia wolności i grzywnie w wysokości 45 tys. euro.

Zgodnie z art. 223-15, jeżeli przestępstwa popełniono za pośrednictwem prasy pisemnej lub audiowizualnej, do ustalenia osób odpowiedzialnych mają zastosowanie szczególne przepisy ustaw regulujących te sprawy.

Artykuł 226-1 dotyczy naruszenia praw autorskich. W myśl tego przepisu każdy podlega karze jednego roku pozbawienia wolności i grzywny w wysokości 45 tys. euro, jeśli w jakikolwiek sposób umyślnie naruszy prywatność innych osób przez przechwytywanie, utrwalanie lub przesyłanie słów wypowiedzianych prywatnie, lub poufnie bez zgody ich autora, utrwalanie lub przesyłanie bez zgody tego ostatniego, wizerunek osoby w miejscu prywatnym. Jeżeli czyny, o których mowa w niniejszym artykule, zostały popełnione na oczach i przy wiedzy zainteresowanych stron, a nie sprzeciwiały się one temu, o ile były one w stanie to uczynić, domniemywa się zgodę tych ostatnich.

Zgodnie z art. 226-2 tej samej karze podlega fakt przechowywania, ujawniania opinii publicznej lub osobie trzeciej bądź wykorzystywania w jakikolwiek sposób nagrania lub dokumentu uzyskanego za pomocą jednej z przewidzianych wcześniej wymienionych czynności. Jeżeli przestępstwo, o którym mowa w poprzednim ustępie, zostało popełnione za pośrednictwem prasy pisemnej lub audiowizualnej, w

odniesieniu do ustalenia osób odpowiedzialnych zastosowanie mają szczególne przepisy ustaw regulujących te sprawy.

Według art. 226-2-1 w sprawie rozpowszechniania pornografii, jeżeli przestępstwa dotyczą słów lub obrazów o charakterze seksualnym wykonanych w miejscu publicznym lub prywatnym, kara wynosi do dwóch lat pozbawienia wolności i grzywny w wysokości 60 tys. euro. Tej samej karze podlega czyn, w przypadku braku zgody osoby na rozpowszechniania do opinii publicznej lub osoby trzeciej jakichkolwiek nagrań bądź dokumentów odnoszących się do słów lub obrazów o charakterze seksualnym uzyskanych za wyraźną lub domniemaną zgodą osoby lub samodzielnie, przy użyciu jednego z czynów przewidzianych w art. 226-1.

Zgodnie z art. 226-3 w sprawie rozprowadzania urządzeń technicznych każdy podlega karze pięciu lat pozbawienia wolności i grzywnie w wysokości 300 tys. euro, jeżeli wytwarza, importuje, posiada, wystawia, oferuje, wynajmuje lub sprzedaje urządzenia techniczne, umożliwiające wykonywanie czynności mogących stanowić przestępstwo art. 226-2 lub które, przeznaczone do zdalnego wykrywania rozmów, umożliwiają dokonanie przestępstwa przewidzianego lub mającego na celu przeciwdziałanie przechwyceniu danych informatycznych przewidzianych w *Kodeksie postępowania karnego* i *Kodeksie bezpieczeństwa wewnętrznego* oraz na liście sporządzonej na warunkach określonych w dekrecie Rady Stanu, a w przypadku popełnienia tych czynów w wyniku zaniedbania, bez upoważnienia ministerialnego, którego warunki przyznawania są określone w tym samym dekrecie lub, bez przestrzegania warunków określonych w niniejszym zezwoleniu; produkuje reklamę dotyczącą urządzenia technicznego, które może pozwolić na popełnienie wykroczeń przewidzianych w art. 226-1 i drugim akapicie art. 226-15, gdy reklama ta stanowi podżeganie do popełnienia tego przestępstwa lub mając za cel przechwytywanie danych komputerowych, o których mowa w art. 706-102-1 i 706-102-2 *Kodeksu postępowania karnego* i L. 853-2 *Kodeksu bezpieczeństwa wewnętrznego*, jeżeli reklama ta stanowi zachętę do jej nieuczciwego wykorzystania.

Wejście do domu innych osób przy użyciu manewrów, gróźb, napaści lub przymusu, z wyjątkiem przypadków, w których zezwala na

to prawo, w myśl art. 226-4 podlega karze pozbawienia wolności i grzywny w wysokości 15 tys. euro. Przebywanie w domu innych osób po wprowadzeniu, o którym mowa w akapicie pierwszym, z wyjątkiem przypadków, w których prawo na to zezwala, podlega takiej samej karze.

Fakt przywłaszczenia sobie tożsamości osoby trzeciej lub wykorzystania jednego lub więcej danych dowolnego rodzaju umożliwiających jej identyfikację w celu zakłócenia spokoju jego lub innych osób bądź podważenia jego honoru lub w jego ocenie, zgodnie z art. 226-4-1 podlega karze roku pozbawienia wolności i grzywny w wysokości 15 tys. euro. To wykroczenie podlega takiej samej karze, gdy zostało popełnione w publicznej sieci komunikacyjnej online.

Zgodnie z art. 226-4-2 zmuszanie osoby trzeciej do opuszczenia miejsca zamieszkania bez uzyskania pomocy państwa na przewidzianych warunkach, za pomocą działania, gróźb, napaści lub przymusu, podlega karze trzech lat pozbawienia wolności i grzywnie w wysokości 30 tys. euro. Według art. 226-5 usiłowanie popełnienia przestępstwa, o którym mowa w tej sekcji, podlega takiej samej karze.

Na podstawie *la loi* nr 2015-912 z dnia 24 lipca 2015 r. dotyczącej informacji mającej na celu stworzenie ram prawnych, spójnych i kompleksowych dla sztucznej inteligencji (AI):

- wprowadzono modyfikację przepisów dotyczących wdrażania przechwytywania zabezpieczeń i dostępu do danych o połączeniach;
- stworzono ramy prawne dla realizacji wdrożenia niektórych technik zbierania informacji, wykrywania słabych sygnałów, wykorzystania ŁAPACZY IMSI, nagłośnienia, robienia i nagrywania zdjęć, danych komputerowych, w tym w pojeździe lub miejscu prywatnym.

System „czarnych skrzynek" (*boîtes noires*) został wprowadzony we Francji na podstawie art. L 851-3 ustawy o wywiadzie[907]. Zgodnie z art. 851-3 kodeksu bezpieczeństwa wewnętrznego po uzyskaniu zgody premiera, wydanej po uzyskaniu zgody Narodowej Komisji Kontroli Technik Pozyskiwania Informacji (CNCTR)[908], operatorzy telekomunikacyjni oraz osoby zajmujące się dostarczaniem usług

komunikacji elektronicznej, wymienione w ustawach kodeks pocztowy i telekomunikacyjny oraz w ustawie o zaufaniu do gospodarki cyfrowej, mogą zostać zobowiązani do wprowadzenia w administrowanych przez nich sieciach automatycznego przetwarzania danych tzw. czarnych skrzynek, w celu wykrycia połączeń mogących wskazywać na zagrożenie terrorystyczne. „Czarne skrzynki" analizują w sposób masowy przepływ danych komunikacyjnych przesyłanych za pośrednictwem kabli optycznych w celu wykrycia. Zbieranie danych w tym trybie musi spełniać kryteria zawarte w autoryzacji określającej w sposób wyczerpujący dane, które mają być pozyskane, oraz ich parametry techniczne. Czynnikiem utrudniającym efektywną realizację zadań służb odpowiedzialnych za wywiad czy bezpieczeństwo wewnętrzne jest coraz większa dywersyfikacja środków komunikacji, zarówno telefonów, jak i komunikatorów internetowych takich jak Skype, Telegram, WhatsApp, Signal czy innych, a także coraz wyższy stopień zaawansowania technologicznego tych urządzeń. Tradycyjne, ukierunkowane metody przechwytywania treści komunikacji określonej osoby nie są dostosowane do współczesnych zagrożeń oraz nie pozwalają na spójne i nieprzerwane prowadzenie czynności operacyjno-rozpoznawczych w sytuacji, gdy określona osoba posługuje się różnymi środkami komunikacji czy zmienia dane umożliwiające jej identyfikację (np. numer telefonu, adres poczty elektronicznej)[909].

Pozyskiwanie przez służby danych informatycznych ma szczególne znaczenie w zapobieganiu i zwalczaniu zagrożeń o charakterze terrorystycznym. Masowe wykorzystywanie nowych środków komunikacji przez takie podmioty, jak tzw. Państwo Islamskie, sprawia, że w kilku ostatnich lat znacznie wzrosła ilość danych (np. zdjęcia, pliki wideo, prywatne wiadomości), których francuskie służby nie mogą zdobyć ze względu na ograniczenia natury technologicznej i prawnej. Przechwytywanie danych informatycznych dotyczących odwiedzanych stron internetowych, metadanych o komunikacji elektronicznej czy danych dotyczących zakupów dokonywanych za pośrednictwem sklepów internetowych jest, według twórców dokumentu, niezbędne do ustalenia np. zamiaru wyjazdu określonej osoby do stref działania ugrupowań terrorystycznych (Syria, Irak).

Pomoże to ujawnić charakterystyczne dla procesu radykalizacji elementy, np. zakup sprzętu paramilitarnego czy utrzymywanie kontaktów z określonymi osobami bądź środowiskami.

Z kolei praktyka orzecznicza w odniesieniu działań podejmowanych w cyberprzestrzeni przyjęła niespójną linię. By w pełni zrozumieć problem wynikający z konieczności stosowania przepisów francuskich obowiązujących w odniesieniu do jurysdykcji w cyberprzestrzeni, należy przytoczyć kilka interesujących orzeczeń poruszających omawianą kwestię[910]. Najbardziej znaną sprawą francuską, która wywołała ogólnoświatową dyskusję na temat granic kompetencji jurysdykcyjnych sądów krajowych, była sprawa Yahoo![911]

Pozew przeciwko internetowemu gigantowi Yahoo! Inc. wytoczyły organizacja LICRA oraz Francuski Związek Studentów Żydowskich. Firma Yahoo! na swojej aukcji internetowej zamieściła przedmioty o tematyce nazistowskiej. Aukcja była dostępna również dla internautów francuskich, zarówno za pomocą amerykańskiej, jak i francuskiej wersji strony. Francuski sędzia uznał, że Yahoo! naruszyło prawo francuskie, które zakazuje wszystkiego, co pobudza nienawiść rasową, i nałożył na amerykańską firmę grzywnę pieniężną za obrazę zbiorowej pamięci Francuzów oraz nakazał zablokowanie dostępu do witryny, na której odbywała się aukcja.

Sąd uznał, że „podczas gdy Yahoo! Inc. pozostawało świadome faktu skierowania swoich działań do podmiotów francuskich, ponieważ dokonując połączenia ze stronami aukcji z terminali znajdujących się we Francji, przekazywało ono ogłoszenia reklamowe w języku francuskim. […] niniejszym ustanowione zostało wystarczające połączenie dla uznania połączenia z Francją, które pozwala naszym sądom uznać się za całkowicie kompetentne do rozstrzygania powierzonej im kwestii”. Sąd francuski oparł swoje rozstrzygnięcie na konieczności obrony porządku publicznego, przestrzegania prawa oraz wartości wspólnym wszystkim narodom, czyli potępienie zbrodni hitlerowskich.

Yahoo! broniło swojego stanowiska, opierając się na pierwszej poprawce do amerykańskiej konstytucji gwarantującej wolność słowa. Mimo złożenia odwołania sąd apelacyjny utrzymał wyrok sądu pierwszej instancji w mocy. Sąd francuski nakazał firmie

amerykańskiej zablokowanie dostępu do witryny, na której widniała aukcja. Yahoo! nie złożyło kasacji od wyroku sądu drugiej instancji, lecz samo złożyło pozew w Stanach Zjednoczonych, licząc na wydanie decyzji potwierdzającej niemożność wykonania orzeczenia francuskiego na amerykańskim terytorium. Amerykański sąd pierwszej instancji uznał powództwo Yahoo! Wyrok został też utrzymany w mocy przez sąd apelacyjny Dziewiątego Okręgu[912], który uznał jurysdykcję sądów amerykańskich do rozstrzygnięcia sporu, lecz mimo nadziei Yahoo! nie orzeczono zakazu wykonania francuskiego wyroku na terytorium USA.

J. Kulesza[913] w rozważaniach na temat sprawy Yahoo! uznała, że „z perspektywy rozważań jurysdykcyjnych sprawa ta stanowi sygnał rozszerzenia stosowanych dotychczas standardów, na podstawie których sądy Stanów Zjednoczonych decydowały się wykonywać uprawnienia jurysdykcyjne wobec spraw z przeważającym elementem obcym. Sprawa ta wydaje się więc sygnałem dla sądów innych państw, że wolno im wykonywać władzę w spawach z minimalnym udziałem podmiotów amerykańskich […]. O ile konsekwencje prawne i jurysdykcyjne są ważne dla omawianej sprawy, o tyle jej aspekt internetowy podkreśla złożoność zależności świata online i tradycyjnych granic". Wyrok sądu francuskiego był szeroko krytykowany w doktrynie. Nie można zgodzić się z poglądem wyrażonym w wyroku, że sam fakt dostępności treści w danym języku był wystarczającym czynnikiem do uznania swojej jurysdykcji. Przyjęcie takiej koncepcji przez wszystkie państwa na świecie i wszystkie porządki prawne mogłoby wprowadzić chaos oraz niepewność obrotu prawnego.

Część orzecznictwa francuskiego uznała kryterium nakierowania przekazu za przesłankę naruszenia prawa z rejestracji znaku towarowego. Sąd apelacyjny w Paryżu w orzeczeniu z dnia 27 września 2006 r.[914] odrzucił kryterium dostępności strony internetowej jako podstawy uznania swojej jurysdykcji. To orzeczenie sprzeczne z wyrokiem w sprawie dotyczącej hiszpańskiego przedsiębiorcy posługującego się na swojej stronie www identycznym znakiem towarowym jak przedsiębiorca francuski. Sąd uznał, że „z uwagi na zredagowanie strony w języku hiszpańskim wraz z umożliwieniem za

jej pośrednictwem dokonywania transakcji w pesetach[915] w żaden sposób nie zostało dowiedzione, że posłużenie się identycznym oznaczeniem do podlegającego ochronie we Francji na stronie internetowej, choć dostępnej we Francji, stanowi wkroczenie w zakres prawa wyłącznego przysługującego na jej terytorium”[916]. Można się spotkać z poglądem, że w internetowych stosunkach handlowych język powinien być kryterium jurysdykcyjnym, który wprowadza domniemanie skierowania treści zawartych na stronie internetowej do odbiorcy krajowego[917]. Innym kryterium może być waluta, oferowane możliwości dostawy czy nazwy domeny. Nie można uznać, że powinien to być główny i jedyny łącznik jurysdykcyjny określający prawo właściwe do rozstrzygnięcia sporu. Język, waluta czy nazwa domeny powinny być stosowane jedynie pomocniczo.

6.4.2. INSTYTUCJONALNY WYMIAR POLITYKI CYBERBEZPIECZEŃSTWA

Francja jest jednym z pierwszych państw, które podjęły działania legislacyjne w celu wzmocnienia swojego cyberbezpieczeństwa w dziedzinie infrastruktury usług kluczowych. Ważne decyzje dotyczące walki z terroryzmem są podejmowane w tym państwie pod przewodnictwem prezydenta Francji oraz Rady Bezpieczeństwa Wewnętrznego (CSI)[918], która definiuje kierunki polityki w dziedzinie bezpieczeństwa wewnętrznego i ustala priorytety. Premier zbiera ministrów zaangażowanych w antyterroryzm. Ich zadaniem jest koordynowanie działań i ustalanie ich kierunków. Politykę państwa w zakresie ochrony systemów teleinformatycznych prowadzi premier za pośrednictwem ANSSI zatrudniającej ok. 500 pracowników. Premier przewodniczy również Międzyresortowemu Komitetowi ds. Wywiadu (CIR)[919], który prowadzi prace dotyczące szkoleń technicznych[920].

Minister spraw wewnętrznych przewodniczy Międzyresortowemu Komitetowi Antyterrorystycznemu (CILAT), który koordynuje działania podjęte podczas planu międzyresortowego. Dyrektor gabinetu premiera przekazuje ministrowi wytyczne nadane przez Prezesa Rady Ministrów w czasie regularnych spotkań dotyczących kwestii bezpieczeństwa narodowego. W Ministerstwie Spraw

Wewnętrznych większość służb specjalnych odpowiedzialnych za działania przeciwko terroryzmowi jest związana z Dyrekcją Generalną Policji Narodowej (DGPN). Od 1 lipca 2008 r. działa Centralna Dyrekcja Wywiadu Krajowego (DCRI), która jest agencją wywiadowczą francuskiego MSW, powstałą z połączenia francuskiej służby kontrwywiadu (DST)[921] i Centralnej Dyrekcji Wywiadu Ogólnego (DCRG)[922]. Połączenie ma tę zaletę, że nowo powstała agencja łączy dwie role: administracyjną, polegającą na monitorowaniu doprowadzenia osób podejrzanych lub grup, i sądową, kiedy sędziowie uczestniczą w śledztwach w sprawach karnych. Centralna Dyrekcja Policji Sądowej (DCPJ) prowadzi liczne dochodzenia przez Narodowy Wydział Antyterrorystyczny (DNAT), znany jako Subagencja Antyterrorystyczna (SDAT). W zakresie przestępstw finansowych specjalistyczne urzędy centralne mogą także współuczestniczyć w prowadzeniu dochodzenia. Oddział Monitorowania i Raportowania (DST), oprócz tradycyjnej misji szpiegowskiej, bezpośrednio przyczynia się do zapobiegania i karania terrorystycznego działania w ramach kompetencji policji i wymiaru sprawiedliwości. Centralna Dyrekcja Informacji Ogólnych jest odpowiedzialna za monitorowanie grup ryzyka[923].

Antyterrorystyczna Jednostka Współpracy (UCLAT), na poziomie operacyjnym jednostka koordynująca walkę z terroryzmem, została utworzona w 1984 r. przy Ministerstwie Spraw Wewnętrznych. Koordynuje wszystkie usługi związane z walką z terroryzmem, dzięki czemu codziennie analizuje i syntezuje informacje o terroryzmie. Ściśle współpracuje z DCRG, Narodową Żandarmerią, DGSE, DGE/CCED i Oddziałem Celnym. Zapewnia wymianę informacji operacyjnych wszystkich organów i służb zaangażowanych w walkę z wszelkimi formami terroryzmu. Zbiera informacje dostarczone przez odpowiednie służby Ministerstwa Spraw Wewnętrznych, Ministerstwa Obrony i Ministerstwa Gospodarki, Finansów i Przemysłu. UCLAT wymienia także regularnie informacje z władzą sądowniczą. Policyjny RAID (Biuro Badań, Pomocy, Interwencji i Zniechęcania) jest zawsze dostępny, aby pomóc DGPN w nagłych wypadkach[924].

ANSSI dzięki pionowi operacyjnemu i rozmieszczonym w ministerstwach sieciach typu honey-pot ma dostęp do bieżącej

informacji na temat ataków i innych zagrożeń na poziomie centralnym, jednocześnie pełni funkcję CSIRT odpowiedzialnego za obsługę incydentów i zagrożeń na szczeblu krajowym CERT-FR (CERT Narodowy).

Do zadań ANSSI, zgodnie z art. 3 dekretu, należy:

- pełnienie funkcji narodowej władzy bezpieczeństwa systemów informatycznych. W tym celu przedkłada ona premierowi propozycje działań zmierzających do reagowania na sytuacje kryzysowe i zagrożenia bezpieczeństwa systemów wykorzystywanych przez organy publiczne, operatorów infrastruktury krytycznej, a także koordynuje, w ramach określonych przez premiera wytycznych, działania rządu w tym zakresie;
- opracowywanie i wdrażanie międzyresortowych bezpiecznych środków komunikacji elektronicznej wykorzystywanych przez prezydenta i rząd;
- inicjowanie i koordynowanie międzyresortowych działań dotyczących bezpieczeństwa systemów informatycznych;
- opracowywanie środków ochrony systemów informatycznych, które następnie są przedstawiane premierowi, oraz nadzorowanie procesu ich stosowania przyjętych środków;
- prowadzenie inspekcji systemów informatycznych wykorzystywanych przez organy administracji publicznej i operatorów infrastruktury krytycznej;
- opracowywanie systemów wykrywania zdarzeń mogących naruszać bezpieczeństwo państwowych systemów informatycznych oraz koordynacja działań, które mają na celu przeciwdziałanie tym zdarzeniom;
- zbieranie informacji technicznych o incydentach dotyczących państwowych systemów informatycznych i operatorów infrastruktury krytycznej;
- wydawanie certyfikatów dopuszczających do użytku urządzenia i mechanizmy techniczne chroniące informacje objęte tzw. tajemnicą obrony;
- udział w negocjacjach międzynarodowych oraz prowadzenie współpracy z zagranicznymi organami pełniącymi analogiczne

funkcje;
- prowadzenie działalności szkoleniowej dla osób zajmujących się problematyką bezpieczeństwa systemów informatycznych.

W myśl art. 4 dekretu Narodowa Agencja Bezpieczeństwa Systemów Informatycznych dokonuje również oceny poziomu bezpieczeństwa urządzeń i usług niezbędnych do ochrony systemów informatycznych. Agencja jest odpowiedzialna przede wszystkim za:
- kwalifikację urządzeń bezpieczeństwa i dostawców usług zaufania;
- wydawanie upoważnień podmiotom, o których mowa w dekrecie nr 2010-112 z 2 lutego 2010 r.;
- kwalifikację urządzeń bezpieczeństwa i dostawców usług zaufania, a także zatwierdzanie punktów ewaluacji przewidzianych w dekrecie nr 2015-350 z 27 marca 2015 r.;
- certyfikację urządzeń służących do generowania i weryfikacji podpisów elektronicznych przewidzianych w dekrecie z 30 marca 2001 r.;
- zatwierdzanie punktów ewaluacji i certyfikacji poziomu bezpieczeństwa urządzeń i systemów informatycznych, o których mowa w dekrecie z 18 kwietnia 2002 r.;
- wydawanie autoryzacji i zarządzanie deklaracjami dotyczącymi środków i dostawców instrumentów kryptologicznych, o których mowa w dekrecie z 2 maja 2007 r.;
- wydawanie i cofanie zezwoleń, o których mowa w art. 226-3 k.k. (zezwolenia na produkcję i sprzedaż urządzeń służących do utrwalania treści rozmów i pozyskiwania danych informatycznych).

SGDSN przedstawia i wdraża politykę rządu francuskiego w zakresie bezpieczeństwa systemów informatycznych, szczególnie w przypadku systemów przetwarzania informacji niejawnych związanych z obroną narodową. Gwarantuje to, że prezydent Republiki Francuskiej oraz rząd dysponują systemami obrony i bezpieczeństwa narodowego niezbędnymi do komunikacji. Bezpieczeństwo cybernetyczne jest nadzorowane w ministerstwach przez HFDS, a w organizacjach niepodlegających ministerstwu jest wymóg zastosowania

niezbędnych, równoznacznych środków bezpieczeństwa. Głównym zadaniem jest zachowanie poufności oraz integralności, proporcjonalnej do wyzwań i wymagań systemowych. Premier powołuje również tzw. Władze Kwalifikowane – *Autorité qualifiée en sécurité des systèmes d'information*. Są one odpowiedzialne za weryfikację poziomu bezpieczeństwa komputerowego na poziomie departamentów i ministerstw. 27 stycznia 2017 r. Guillaume Poupard, dyrektor generalny ANSSI, oraz Thierry Delville, delegat ds. bezpieczeństwa i zwalczania zagrożeń cybernetycznych, ogłosili utworzenie *Actions Contre la Cybermalveillance* (ACYMA) – Działania Przeciwko Cyberzłośliwości. Jest to nowy krajowy system pomocy (platforma online) dla ofiar ataków cybernetycznych. Rosnąca liczba ataków komputerowych, chęć poprawy działających systemów oraz nowe narzędzie do pomocy ofiarom ataków cybernetycznych były impulsem do utworzenia ACYMA. To efekt współpracy ANNSI i Ministerstwa Spraw Wewnętrznych. Wszechobecność technologii informacyjnych w życiu społecznym i gospodarczym jest związana ze zwiększonym narażeniem na różnego rodzaju ataki systemów informatycznych. Krajowa Agencja Bezpieczeństwa Systemów Informacyjnych jest centrum francuskiej strategii reagowania na te zagrożenia i odgrywa kluczową rolę w zakresie funkcjonowania i rozbudowy. Prawie 80% agentów pracujących w ANSSI ma tytuł inżyniera lub doktora, przeważnie w dziedzinie informatyki, kryptologii lub matematyki. Agencja funkcjonuje bez przerwy, analizując potencjalne zagrożenia. Republika Francuska z roku na rok jest coraz bardziej atakowana. SGDSN zanotowało ok. 2000 ataków cybernetycznych w 2014 r. oraz ok. 4000 ataków cybernetycznych w 2015 r. Ponadto w 2015 r. SGDSN zainicjowało trzy projekty do walki z dronami[925].

6.5
IMPLEMENTACJA POLITYKI CYBERBEZPIECZEŃSTWA W WIELKIEJ BRYTANII

6.5.1. PODSTAWOWE DOKUMENTY W ZAKRESIE POLITYKI CYBERBEZPIECZEŃSTWA

Rosnące zagrożenie w cyberprzestrzeni zmusiło brytyjski rząd do strategicznego podejścia do tej problematyki. *Pierwsza Strategia Cyberbezpieczeństwa Wielkiej Brytanii* powstała 25 czerwca 2009 r[926]. Grupą, która stanowi dla Wielkiej Brytanii zagrożenie, są cyberterroryści, ponieważ używają oni Internetu głównie do koordynowania działań, szerzenia radykalnej ideologii, zbierania funduszy, a nie do przeprowadzania ataków. Autorzy wskazują, że może to w przyszłości ulec zmianie, ale obecnie terroryści preferują uderzenia klasyczne, ponieważ są zdecydowanie bardziej spektakularne. Najważniejszym elementem strategii z 2009 r. były sugerowane kroki, które brytyjski rząd powinien podjąć w celu przeciwdziałania cyberzagrożeniom. Wskazywano tutaj na konieczność wielopłaszczyznowego podejścia obejmującego ścisłą współpracę rządu, sektora prywatnego oraz środowisk naukowych. Podkreślono też konieczność kooperacji z międzynarodowymi partnerami. W strategii poświęcono też nieco miejsca na działania ofensywne. Autorzy zauważyli, że cyberprzestrzeń może być wykorzystywana do walki z przestępcami i terroryzmem, a nawet przez wojsko, ale aspekt ten w dokumencie nie został rozwinięty[927]

Kolejnym aktem prawnym w Wielkiej Brytanii była strategia bezpieczeństwa narodowego z dnia 18 października 2010 r.[928] *Silna Wielka Brytania w dobie niepewności*. Dokument mówił o stworzeniu strategii cyberbezpieczeństwa. Wynikało to z faktu, że poprzedni dokument był krytykowany i nie spełniał oczekiwań. Nowa strategia została opublikowana pod nazwą *Strategia Cyberbezpieczeństwa Wielkiej Brytanii. Ochrona i wsparcie dla Wielkiej Brytanii w cyfrowym świecie*. Twórcy dokumentu zaznaczyli, że w zglobalizowanym świecie nie można mówić o czymś takim jak absolutne bezpieczeństwo w

cyberprzestrzeni. Zaproponowano podejście polegające na minimalizacji ryzyka. Słusznie dostrzeżono, że rząd Wielkiej Brytanii ma ograniczone pole manewru w cyberprzestrzeni z dwóch powodów: jest ona w dużej części używana przez sektor prywatny i ma charakter transnarodowy. Stąd też wynika potrzeba pracy z przedsiębiorstwami oraz partnerami międzynarodowymi. Kluczowym aspektem nowego dokumentu była wizja Wielkiej Brytanii w 2015 r. jako państwa, które czerpie zyski zarówno ekonomiczne, jak i społeczne z bezpiecznego użytkowania cyberprzestrzeni. W 2015 r. Wielka Brytania miała być w stanie przeprowadzić działania ofensywne w odpowiedzi na zagrożenia w cyberprzestrzeni. Dokument wyznacza również rolę dla przedsiębiorców, którzy w 2015 r. powinni być świadomi zagrożeń w cyberprzestrzeni. Miało to doprowadzić do sytuacji, w której wrażliwe informacje są przekazywane z zachowaniem należytych środków bezpieczeństwa. Bliska współpraca sektora prywatnego z publicznym przez wymianę wartościowych danych miała przyczynić się do skutecznego zwalczania zagrożeń cybernetycznych.

Strategia bezpieczeństwa cybernetycznego została opublikowana 25 listopada 2011 r.[929] i przyjęta na lata 2011–2016. Kładzie duży nacisk na czynnik ekonomiczny i społeczny, skupiając się na ochronie gospodarki i porządku społecznego. Czynnik militarny, wliczając w to zdolności ofensywne, po raz kolejny został zaniedbany. Ciekawym i zarazem ryzykowanym pomysłem była idea zaangażowania społeczności brytyjskiej w ochronę w cyberprzestrzeni. Według zawartej w niej definicji: „Cyberprzestrzeń to interaktywna domena stworzona z cyfrowych sieci, która jest wykorzystywana do przechowywania, modyfikowania oraz przekazywania informacji". Jej częścią jest Internet, ale zawierają się w niej także inne systemy informacyjne, które obsługują biznes, infrastrukturę oraz wspomagają świadczenie usług. Cyfrowe sieci już dziś podbudowują proces zaopatrywania domów w energię elektryczną oraz wodę, pomagają organizować dostawy żywności oraz innych dóbr do sklepów i służą za niezbędne narzędzie biznesowe w całym Zjednoczonym Królestwie.

W przytoczonej definicji do zakresu przedmiotowego cyberprzestrzeni oprócz Internetu włączono także inne sieci, niekoniecznie połączone z globalną siecią www, np. lokalne

wykorzystywane w dużych przedsiębiorstwach. Wprowadzając pojęcie interaktywności, autorzy definicji podkreślili także istotną cechę sieci komputerowych, które są dla swoich użytkowników nie tylko źródłem informacji, lecz także obszarem podlegającym kształtowaniu przez swoich odbiorców.

W drodze do zrealizowania wizji bezpieczeństwa cybernetycznego Wielkiej Brytanii na lata 2011–2016[930] wyodrębniono cztery główne cele. Pierwszy to skuteczne zwalczanie cyberprzestępczości i uczynienie z Wielkiej Brytanii najbezpieczniejszego miejsca na świecie do prowadzenia działalności gospodarczej w cyberprzestrzeni. Cel ten miał zostać osiągnięty przez zmniejszenie podatności brytyjskich sieci na ataki, ograniczenie działalności cyberprzestępców oraz promocję skutecznego partnerstwa między sektorami prywatnym a publicznym. Sugerowano również konieczność zwiększenia świadomości społecznej na temat ataków, ulepszenie mechanizmu reagowania na incydenty, lepszą ochronę kluczowych informacji i usług, promowanie zaufania w cyberprzestrzeni. Proponowano nałożenie sankcji na osoby ją propagujące, zacieśnianie współpracy z przedsiębiorstwami przy wdrażaniu nowego prawa, które ma nie przeszkadzać w swobodnej wymianie informacji, a zarazem przewidywać poważne kary dla cyberprzestępców. Założono współpracę z międzynarodowymi organizacjami oraz innymi państwami w celu opracowywania i wdrażania transgranicznych rozwiązań prawnych, które zapobiegną sytuacji tworzenia się bezpiecznych przystani dla cyberkryminalistów.

Drugim celem miało być uczynienie Wielkiej Brytanii bardziej odpornej na ataki cybernetyczne oraz zagwarantowanie skuteczniejszej obrony brytyjskich interesów w cyberprzestrzeni. Za najważniejsze w realizacji tego długoterminowego celu rząd postawił sobie wzmocnienie obrony w cyberprzestrzeni oraz odporności na ataki, a także zmniejszenie siły ich oddziaływania oraz przeciwdziałania w celu wykorzystywaniu sieci przez terrorystów. Co więcej, zapowiedziano działania mające na celu udoskonalenie wykrywania zagrożeń w cyberprzestrzeni oraz wzmocnienie zdolności do powstrzymywania i neutralizowania ataków hakerskich przez zacieśnienie współpracy z przedsiębiorstwami odpowiedzialnymi za

kierowanie systemami infrastruktury krytycznej. Planowano implementację polityki bezpieczeństwa w cyberprzestrzeni opracowanej przez NATO i utworzenie grup operacyjnych w ramach Ministerstwa Obronny, które będą odpowiedzialne za integrację potencjałów cywilnych i wojskowych w cyberprzestrzeni.

Kolejnym celem była praca na rzecz kształtowania otwartej i stabilnej cyberprzestrzeni, która może być używana w bezpieczny sposób przez społeczeństwo Wielkiej Brytanii. Realizując ten cel, rząd zamierzał oprzeć się na promowaniu otwartej cyberprzestrzeni, gdzie zapewnienie bezpieczeństwa nie ma negatywnego wpływu na prawo wolności internautów. W szczegółowym planie działań wymieniono:

- kontynuowanie organizowania międzynarodowych konferencji poświęconych ustanowieniu międzynarodowych norm co do zachowania się w cyberprzestrzeni;
- przegląd istniejących przepisów dotyczących sektora komunikacyjnego w Wielkiej Brytanii;
- implementację bilateralnych umów ze Stanami Zjednoczonymi, Francją i Australią;
- szukanie porozumienia z państwami rozwijającymi się, które aktywnie angażują się w działalność w cyberprzestrzeni;
- aktywne zaangażowanie się w pracę organizacji międzynarodowych i regionalnych, takich jak OBWE, Rada Europy i Międzynarodowy Związek Telekomunikacyjnym w celu zbudowania jednego modelu legislacyjnego definiującego zachowanie w cyberprzestrzeni;
- współpraca w ramach UE z Komisją Europejską oraz Służbą Działań Zewnętrznych w celu wzmocnienia spójności w działaniach w cyberprzestrzeni;
- próby szukania porozumienia z dostawcami Internetu w celu współpracy w identyfikacji złośliwego oprogramowania.

Czwartym celem było wykształcenie wybitnych ekspertów w dziedzinie cyberbezpieczeństwa Wielkiej Brytanii. Miał on zostać osiągnięty przez stworzenie wspólnego programu badawczego, w którego ramach będą pracowali specjaliści z wielu dziedzin. Ma on obejmować działania mające na celu lepsze zrozumienie zagrożeń i

ryzyka operowania w cyberprzestrzeni, jak również umożliwić łatwiejsze znalezienie wrażliwych punktów. Bardzo ważnym aspektem jest uświadomienie społeczeństwu ryzyka, jakie wiąże się z użytkowaniem cyberprzestrzeni, przeprowadzenie specjalnych programów adresowanych do uczniów i studentów oraz ustanowienie specjalnego programu, który miałby służyć za pole ćwiczeń do zwalczania zagrożeń w cyberprzestrzeni z rocznym budżetem 2 mln funtów.

Strategia bezpieczeństwa cybernetycznego na lata 2016–2021 została opublikowana 30 listopada 2016 r.[931] Opiera się na trzech podstawowych celach: powstrzymania cyberagresji, obrony UK przed cyberterroryzmem i rozwoju sektora przemysłowego cyberbezpieczeństwa. Zakłada, że będzie to możliwe dzięki realizacji aż 13 celów szczegółowych:

- zrozumienie zagrożenia zakłada zapewnienie Wielkiej Brytanii zdolność do skutecznego wykrywania, badania i przeciwdziałania zagrożeniu, jakim jest cyberterroryzm;
- zwalczanie cyberprzestępczości – podstawowym założeniem jest ograniczenie wpływu cyberprzestępczości na Wielką Brytanię i jej interesy po to, aby cyberprzestępcy zostali odstraszani od dokonywania ataków;
- reagowanie na incydenty cybernetyczne ma zapewnić możliwość efektywnego zarządzania i reagowania na incydenty cybernetyczne przez zmniejszanie szkody, jakie wyrządzają Wielkiej Brytanii swoimi atakami cyberprzestępcy, i opracowanie skutecznej polityki zwalczania cyberterroryzmu;
- aktywną cyberobronę, której celem jest współpraca z przemysłem, po to, aby osiągnąć skuteczną cyberobronę, ponieważ zmniejszenie skali phishingu i ataków malware nie jest już skuteczne;
- zapewnianie bezpieczeństwa technologii, aby Wielka Brytania była bezpieczniejsza dla produktów i usług technologicznych mających cyberzabezpieczenia;
- poprawa bezpieczeństwa cybernetycznego rządu – sieci rządowe i usługi będą tak bezpieczne, jak to tylko możliwe od momentu ich pierwszego wdrożenia, społeczeństwo będzie mogło korzystać z

rządowych usług cyfrowych po to, aby uzyskać pewność i zaufanie, że ich informacje są bezpieczne;

- zarządzanie ryzykiem cybernetycznym dla gospodarki i społeczeństwa w szerszym ujęciu – wszystkie organizacje w Wielkiej Brytanii, duże i małe, skutecznie zarządzają swoimi ryzykiem cybernetycznym, poparte wysokiej jakości poradami zaprojektowanymi przez NCSC;
- rozwój sektora cyberbezpieczeństwa, którego celem jest zapewnienie, że istnieje prawo do ekosystemu w Wielkiej Brytanii w celu rozwoju i utrzymania cyberprzestrzeni, a sektor bezpieczeństwa może sprostać wymaganiom bezpieczeństwa narodowego;
- rozwój umiejętności w cyberbezpieczeństwie – celem jest zapewnienie Wielkiej Brytanii zrównoważonego transferu rodzimych specjalistów w dziedzinie cyberprzestrzeni, aby sprostać rosnącym wymaganiom coraz bardziej cyfrowej gospodarki w sektorach publicznym i prywatnym oraz obronności;
- badania, rozwój i planowanie przyszłości – celem jest, aby Wielka Brytania została uznana za światowego lidera w dziedzinie bezpieczeństwa cybernetycznego w badaniach i rozwoju, popartego wysokim poziom wiedzy w brytyjskim przemyśle i środowisku akademickim;
- współpraca międzynarodowa – celem jest, aby zagrożenie ataku w cyberprzestrzeni zmniejszało się z powodu wzrostu międzynarodowego konsensusu i zdolności do odpowiedzialnego zachowania państwa w wolnej, otwartej i bezpiecznej cyberprzestrzeni;
- wzmocnienie podejścia społeczeństwa do rządu – celem jest zapewnienie dla rządu, aby zasady organizacji i struktury były uproszczone w taki sposób, aby zmaksymalizować spójność i skuteczność działania na zagrożenie cybernetyczne[932].

Zgodnie ze strategią pojęcie cyberbezpieczeństwa odnosi się do ochrony informacji, systemów (sprzęt, oprogramowanie i infrastruktura towarzysząca), danych na nich zgromadzonych i

świadczonych przez nie usług przed nieautoryzowanym dostępem, uszkodzeniem lub niewłaściwym użyciem. Obejmuje to szkody spowodowane umyślnie lub przypadkowo. Rozszerzono znaczenie cyberprzestrzeni w stosunku do definicji zawartej w strategii z 2011 r., która oznacza „współzależną sieć infrastruktury technologii informacyjnej obejmującą Internet, telekomunikację, sieci, systemy komputerowe, urządzenia połączone z Internetem i urządzenia wbudowane oraz podmioty przetwarzające i administratorów. Może się również odnosić do wirtualnego świata lub domeny jako zjawiska bądź pojęcia abstrakcyjnego".

Pierwszym aktem prawnym regulującym kwestię przestępstw popełnianych przy użyciu komputera był *Computer Misuse Act*[933] z 1990 r. Ustawa powstała jako inicjatywa oddolna, która z czasem zdobyła poparcie rządu i stała się pełnoprawnym aktem prawnym. Wprowadziła penalizację trzech rodzajów przestępstw przeciwko integralności systemów komputerowych. Pierwszy to nieuprawniony dostęp do danych komputerowych, drugi – nieuprawniony dostęp do danych komputerowych z zamiarem popełnienia lub ułatwienia popełnienia innego przestępstwa, trzecim rodzajem przestępstwa jest nieuprawniona zmiana danych komputerowych.

W związku z szybkim rozwojem Internetu i pojawieniem się nowych metod popełniania przestępstw w lipcu 2003 r. rząd brytyjski zreformował *Computer Misuse Act*. W przypadku przestępstw transnarodowych jurysdykcja uzależniona jest od wystąpienia wystarczającego związku (*significiant link*) z „krajem macierzystym, krajem pochodzenia", czyli Anglią, Walią lub Irlandią Północną. W przypadku popełnienia przestępstwa uzyskania nieuprawnionego dostępu do danych komputerowych za wystarczający związek uznaje się jest fakt, że oskarżony był w kraju pochodzenia w chwili popełnienia czynu nieuprawnionego dostępu do komputera, komputer zawierający dane lub program zabezpieczający przed nieuprawnionym dostępem znajdował się w kraju pochodzenia w czasie popełnienia czynu.

Działania mające na celu zapobieganie cyberprzestępczości i innym rodzajom przestępstw są prowadzone również na podstawie wielu przepisów prawnych, w szczególności *Regulation of Investigatory*

Powers Act 2000, oraz zgodnie z odpowiednimi przepisami i konwencjami UE. Istnieje zatem dużo działań związanych z terroryzmem, które mogą mieć miejsce w cyberprzestrzeni, a które są niezgodne z prawem w Wielkiej Brytanii, takich jak rozpowszechnianie publikacji terrorystycznych lub zachęcanie do terroryzmu, ale ich nielegalność nie ogranicza się do ich odbywania się w cyberprzestrzeni. Wykrywanie i monitorowanie jest prowadzone przez liczne organizacje i właściwe organy zgodnie z ich funkcjami i uprawnieniami w ramach strategii i prawodawstwa Wielkiej Brytanii w zakresie zwalczania terroryzmu, przestępstw itp. W Wielkiej Brytanii istnieją przepisy dotyczące działań przeciwko osobom, które nielegalnie prowadzą lub uczestniczą w witrynach internetowych.

Kolejnym aktem prawnym regulującym tę materię w Wielkiej Brytanii jest *Investigatory Powers Act 2016*[934]*,* a konkretnie instrument o nazwie *Bulk Equipment Interference* zawarty w rozdziale 3 części 6 *Investigatory Powers Act* w sekcji 176 i nast. tej ustawy. Pojęcie *Bulk Equipment Interference* (dalej: *bulk)* oznacza nakaz wydany osobie w celu przeprowadzenia działań polegających na ingerencji w funkcjonowanie jakiegokolwiek urządzenia, aby uzyskać treści komunikatów, danych o urządzeniu lub jakichkolwiek innych informacji. Sekcja 176(c) wskazuje natomiast, że głównym celem nakazu powinno być pozyskiwanie informacji, jeżeli wykazują one powiązania zagraniczne. Do najważniejszych elementów należy zaliczyć dwuetapowy proces zatwierdzania nakazu przez Sekretarza Stanu i Komisarza (tzw. *double lock*) oraz wymóg wykazania proporcjonalności i niezbędności wydania nakazu w danym przypadku (sekcja 178).

Te czynności mogą być prowadzone w sposób zdalny lub bezpośredni, np. przez fizyczne wpływanie na działalność danego urządzenia. Mniej skomplikowane działania mogą polegać np. na zgraniu określonych danych z urządzenia czy wykorzystaniu hasła lub loginu użytkownika w celu uzyskania dostępu do informacji zapisanych w pamięci urządzenia. Większy stopień złożoności wykazują działania polegające na wykorzystywaniu słabych punktów określonego oprogramowania służące przejęciu kontroli nad urządzeniem lub siecią, co umożliwia zdalne przekazywanie za ich

pośrednictwem określonych informacji lub monitorowanie aktywności użytkownika. W najbardziej powszechnym rozumieniu ten mechanizm można określić jako prowadzenie czynności o charakterze hakerskim przez służby specjalne[935].

Rolą *bulk* jest przyczynienie się do neutralizacji zagrożenia przez monitorowanie sposobu wykorzystywania urządzeń teleinformatycznych będących prawdopodobnie głównym miejscem działań grupy. Wykrycie osób zaangażowanych w opisane działania wymaga jednak ingerencji we wszystkie urządzenia znajdujące się w danym obiekcie. Przydatność *bulk* wynika w tym przypadku z potencjalnie wysokiej skuteczności tego mechanizmu w sytuacjach dynamicznych, w których uwarunkowania operacyjne podlegają częstym fluktuacjom. Niemożliwe jest bowiem utworzenie wyczerpującej listy podmiotów, do których trafił zainfekowany sprzęt informatyczny lub złośliwe oprogramowanie. Niemożliwe jest również, bez dokładnej znajomości sposobu działania tego oprogramowania, precyzyjne oszacowanie szkód, na jakie są narażone brytyjskie podmioty, i określenia, jakie informacje trafiły do obcych służb.

TABELA 6.1. Odsetek przestępstw według rodzaju w Anglii i w Walii (stan na 25 lutego 2019 r.)

Anglia i Walia			**Dorośli i młodzież powyżej 16. roku życia**
Typ przestępstwa	**Cyberprzestępstwo**	**Niecyberprzestępstwo**	**Łączna liczba przypadków**
Przemoc	0	100	602
Rozbój	4	96	84
Kradzież	0	100	3654
Szkoda kryminalna	0	100	1183

Źródło: https://www.ons.gov.uk/ (dostęp: 15.08.2020).

Dane zamieszczone w tabeli 6.1 potwierdzą, że zarówno polityka Wielkiej Brytanii, jak i instrumenty prawne typu *Bulk Equipment Interference* oraz strategia z 2016 r. w zakresie ochrony

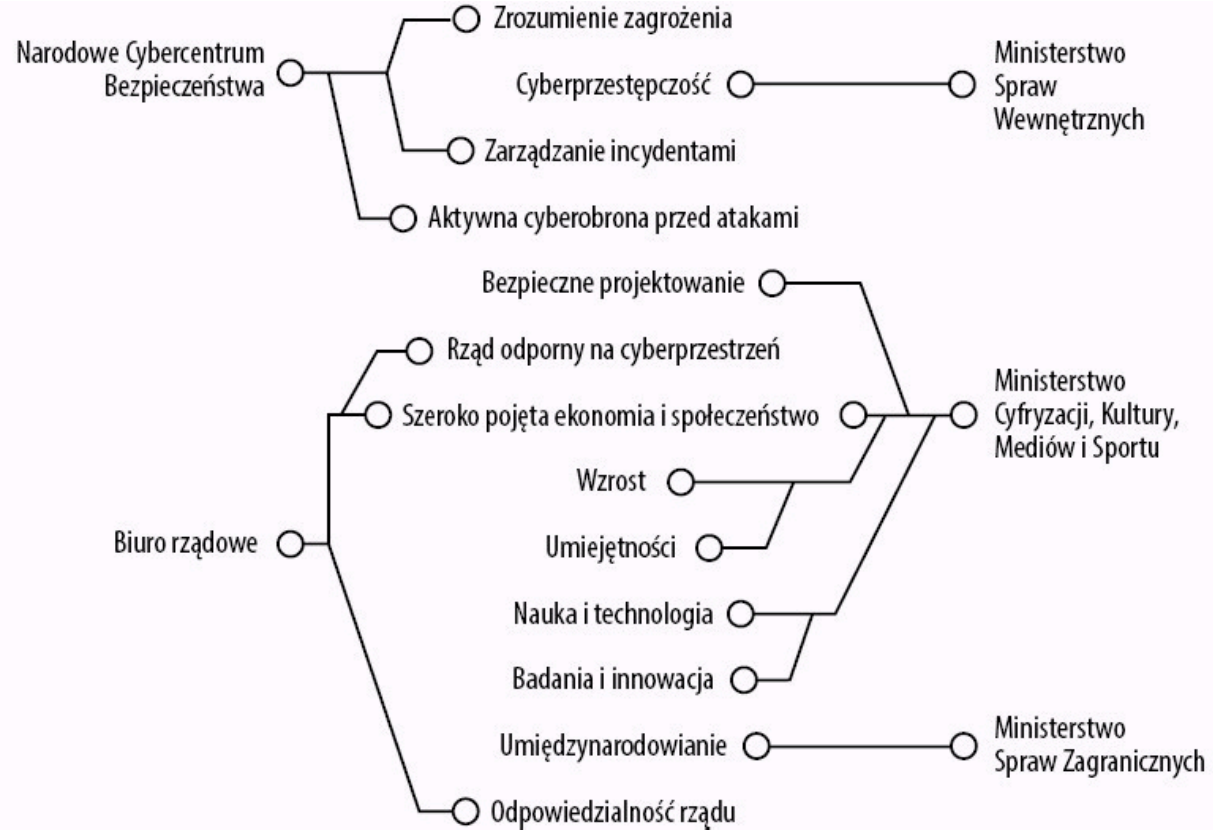
cyberprzestrzeni stawiają na prewencję, co jest dobrym środkiem, aby stać się ważnym graczem (supermocarstwem) w cyberprzestrzeni. Ponadto, w świetle angielskiego orzecznictwa, można zauważyć, że z jednej strony w stosunku do przestępstw polegających na naruszeniu integralności komputera (*computer integrity crimes*) i pozostałych przestępstw popełnianych z wykorzystaniem komputera (*computer – related crimes*) zauważalna jest tendencja do rozszerzenia zakresu obowiązywania angielskiego prawa z wykorzystaniem zasady terytorialnej. Na tym tle pojawia się ryzyko dynamicznej interpretacji *actus reus* i karania nieświadomych obcokrajowców, jedynie na podstawie natury środowiska technologicznego, z którego korzystają. Z drugiej strony angielskie sądy z reguły nie zajmują się sprawami przestępstw popełnianych poza granicami Anglii i Walii, nawet gdy sprawcą przestępstwa jest obywatel brytyjski. Odstępstwa od tej zasady są wyjątkowe i mają charakter ustawowy[936].

Jedną z pierwszych spraw, w której został podniesiony problem jurysdykcji w Internecie, była sprawa oszustwa na szkodę amerykańskiego Citibanku[937]. W 1994 r. bank ten stał się ofiarą cyberprzestępców, którzy zdołali przelać na swoje konto z rachunków klientów banku kwotę ok. 12 mln dolarów. Po przeprowadzeniu śledztwa i dzięki międzynarodowej współpracy organów ścigania zidentyfikowano sprawcę. Władimir Levin został aresztowany w Anglii i mimo składanych apelacji dokonano jego ekstradycji na terytorium Stanów Zjednoczonych.

Podstawowym problemem w sprawie Levina była kwestia konfliktu jurysdykcyjnego kilku państw. Obrońca oskarżonego twierdził, że czyn został popełniony w Rosji, ponieważ sprawca, przebywając w Sankt Petersburgu, wprowadził do swojego komputera program, który umożliwił dokonanie oszustwa. Dlatego – w opinii obrońcy Levina – sąd brytyjski powinien zastosować prawo rosyjskie. Z kolei pełnomocnik popierający amerykański wniosek ekstradycyjny twierdził, że przestępstwo miało miejsce tam, gdzie nastąpiły zmiany w systemie komputerowym Citibanku, czyli w Parsippany, w stanie New Jersey, USA. Sędzia przychylił się do wniosku ekstradycyjnego, argumentując, że podejrzany, wprowadzając na swoim komputerze program w czasie rzeczywistym, spowodował skutek w serwerach

Citibanku. Sąd uznał zatem, że czyn popełniono w miejscu wystąpienia skutku przestępstwa (*termination*).

6.5.2. INSTYTUCJONALNY WYMIAR POLITYKI CYBERBEZPIECZEŃSTWA



RYSUNEK 6.11
Instytucjonalny podział obowiązków w obszarze strategii cyberbezpieczeństwa w Wielkiej Brytanii

Źródło: Raport z postępów działań w ramach cyberstrategii 2016–2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/805677/National_Cyber_Security_Strategy_Progress_Report.pdf (dostęp: 30.07.2020).

Secret Intelligence Service (SIS) jest regulowany przez ustawę o tej samej nazwie z 1994 r., dotyczącą gromadzenia obcych tajnych danych, w interesie bezpieczeństwa narodowego, a w odniesieniu do obrony i polityki zagranicznej podyktowanej interesem dobrobytu gospodarczego w Wielkiej Brytanii i na rzecz zapobiegania poważnym

przestępstwom. *The Government Communications Headquarters* (GCHQ) uregulowany w ustawie z 1994 r., daje możliwość przeciwstawiania się licznym zagrożeniom, w tym terroryzmowi. Jest to również krajowy organ techniczny zapewniający źródło informacji, pomagający rządowi zachować bezpieczny system komunikacji i teleinformacji przed hakerami i innymi zagrożeniami.

Sekcja Współpracy Międzynarodowej (ILS) jest punktem kontaktowym policji obywatelskiej w celu wymiany informacji i danych wywiadowczych w sprawie terroryzmu między brytyjską policją a europejskimi i międzynarodowymi agencjami policyjnymi. Posiada antyterrorystycznych oficerów łącznikowych w wielu stolicach.

The Metropolitan Police Special Branch i The Metropolitan Police's Anti-Terrorist Branch połączyły się, tworząc Komendę Antyterrorystyczną (CTC). CTC ponosi odpowiedzialność i wydaje ekspertyzy dla badań reaktywnych i proaktywnych śledztwa, może także zostać wezwana przez innych głównych urzędników lub władze NCTI do pomocy w śledztwie terrorystycznym na zewnątrz. CTC i Security Service współpracują w celu zapewnienia, że wywiad maksymalnie przeciwdziała terroryzmowi[938].

W strategii z 2009 r. zadecydowano o powołaniu Biura Cyberbezpieczeństwa, którego głównym zadaniem miało być koordynowanie działań w cyberprzestrzeni oraz opracowywanie strategii. Utworzono też Centrum Operacji Cybernetycznych do monitorowania sytuacji w cyberprzestrzeni, lepszego zrozumienia natury ataków, które są wymierzone w Wielką Brytanię, oraz zapewnienia łatwego dostępu do informacji dla sektorów prywatnego i publicznego[939]. Centrum to mieści się w Cheltenham i jest jednym z elementów Centrali Łączności Rządowej (GCHQ), która jest brytyjską służbą specjalną zajmującą się wywiadem elektronicznym i jest odpowiedzialna za zbieranie oraz analizę informacji pochodzących m.in. z cyberprzestrzeni (*Keeping our Society Safe and Successful in the Internet Age*).

W lutym 2017 r. w Wielkiej Brytanii została zainagurowana działalność Narodowego Centrum Cyberbezpieczeństwa (National Cyber Security Centre – NCSC). Zadaniem Centrum jest pomoc

administracji publicznej i przedsiębiorstwom w reagowaniu na poważne incydenty w dziedzinie cyberbezpieczeństwa oraz zwiększenie bezpieczeństwa w Internecie dzięki działalności doradczej oraz pomocy technicznej. Przykładowe działania obejmują przeszukiwanie luk w zabezpieczeniach stron internetowych sektora publicznego czy blokowanie fałszywych e-maili w celu zapobiegania atakom phishingowym.

Organizacyjnie NCSC jest częścią brytyjskiej agencji wywiadu i bezpieczeństwa (Government Communications Headquarters – GCHQ). Zostało powołane w celu implementacji dyrektywy 2016/1148 i pełni funkcję punktu kontaktowego. Koszty uruchomienia i funkcjonowania NCSC do 2020 r., w tym koszty organizacyjne i zatrudnienia 100 najlepszych specjalistów z zakresu cyberbezpieczeństwa, którzy wcześniej pracowali w prywatnych przedsiębiorstwach, wynosi 1,9 mld funtów.

Powołanie NCSC jest kolejnym etapem rozbudowy systemu cyberbezpieczeństwa w Wielkiej Brytanii. Do tej pory kluczową instytucją w systemie był CERT-UK liczący ok. 55 pracowników i realizujący typowe zadania dla CERT/CSIRT, czyli zarządzanie krajowymi incydentami z zakresu cyberbezpieczeństwa, w tym wsparcie dla podmiotów dotkniętych incydentami, oraz promowanie świadomości dotyczącej zagrożeń w cyberprzestrzeni. Funkcjonują również partnerstwa publiczno-prywatne, polegające na wymianie informacji na temat zagrożeń i luk bezpieczeństwa w systemach teleinformatycznych (*Cyber-security Information Sharing Partnership* – inicjatywa CERT-UK) oraz mniejsze, kilkunastoosobowe zespoły analityczne, np. Fusion Cell złożony z przedstawicieli rządu i służb państwowych (pracowników m.in. GCHQ, MI5, MI6 i Policji). Biorąc pod uwagę system prawa w Wielkiej Brytanii, rolą NCSC jest zachęcanie organizacji do zarządzania własnym ryzykiem w zakresie cyberbezpieczeństwa. Centrum wydaje rekomendacje, wytyczne i zapewnia wsparcie dotyczące cyberbezpieczeństwa, w tym w zakresie zarządzania incydentami.

* * *

Analiza prawa ochrony cyberprzestrzeni w wybranych państwach UE pozwoliła ukazać, w jak różny sposób i z jak różną efektywnością oraz szczegółowością można uregulować tę samą problematykę na szczeblu państwowym, będąc członkiem tej samej organizacji międzynarodowej, jaką jest UE i jednocześnie – stroną tych samych konwencji międzynarodowych.

Polityka cyberbezpieczeństwa jest więc wielopłaszczyznowym zjawiskiem, na które składają się różne procesy i czynniki tworzące również ramy kultury politycznej[940]. Jest ona tworzona od każdego prywatnego użytkownika komputera, przez specjalistów ds. bezpieczeństwa cybernetycznego, po programistów, konsultantów oraz organy i organizacje, które w znacznej części przenoszą swoją działalność w wymiar cybernetyczny[941].

Cybertechnologia zmieniła stosunki między państwami oraz sposób prowadzenia rywalizacji politycznej[942]. Państwa nie chcą lub nie są w stanie angażować się w sposób całkowity w prowadzenie wojny, ograniczają więc swoje działania do przestrzeni wirtualnej. Międzynarodowe interakcje cybernetyczne zależą od czynników politycznych, dlatego zjawiska zachodzące w cyberprzestrzeni mogą stanowić odbicie bądź pokłosie realnych działań politycznych. Cyberprzestrzeń można zatem potraktować jako narzędzie do prowadzenia dyplomacji i interakcji międzynarodowych, podobnie jak inne formy nacisków, które posiadają władze państwa[943].

Podsumowując, pierwsze cyberataki o charakterze quasi-militarnym i uznane jako takie zostały przeprowadzone w 2007 r. i 2008 r. przeciwko Estonii, a następnie przeciwko Gruzji. Stały się one przyczyną do podjęcia zmian legislacyjnych w obszarze polityki cyberprzestrzeni zarówno na poziomie unijnym, jak i na poziomie państw członkowskich. Unaoczniły one, że małe państwo, np. Estonia jest zupełnie bezbronne wobec cyberterroryzmu czy też innych form zmasowanej informatycznej napaści. Wydarzenia z Estonii udowodniły, że NATO pozostało bezsilne wobec tych nowych zagrożeń. Problem jest tym istotniejszy, że incydenty tego typu, dzięki swojej zróżnicowanej i stale ewoluującej formie, mogą potencjalnie mieć skutki podobne do osiąganych przy wykorzystaniu konwencjonalnego uzbrojenia. Mimo że ataki nie spowodowały

znacznych szkód materialnych i realnego zagrożenia dla infrastruktury krytycznej, efekt psychologiczny był ogromny. Rząd estoński wyciągnął prawidłowe wnioski z omawianego incydentu, wprowadzając wiele nowych rozwiązań i uregulowań prawnych w różnych dziedzinach bezpieczeństwa, czego najlepszym przykładem jest obecna *Strategia bezpieczeństwa Estonii*. Można zaryzykować tezę, że atak stał się przyczyną do wkroczenia na bardziej zaawansowany prawnie etap estońskiej polityki cyberbezpieczeństwa.

Analiza estońskiego porządku prawnego prowadzi natomiast do przekonania, że władze podejmują właściwe kroki w celu zapewniania bezpiecznego funkcjonowania społeczeństwa obywatelskiego. By spełnić ten warunek, musi być ono kompleksowo uregulowane prawnie w kilku dziedzinach. Estońskie ramy prawne dotyczące cyberprzestrzeni angażują prawo karne, regulacje dotyczące zarządzania kryzysowego i prawa konfliktów zbrojnych. Doświadczenia estońskie ukazują, że konieczne jest ustanowienie wspólnych standardów bezpieczeństwa dla wszystkich użytkowników sieci, systemów i firm zarządzających infrastrukturą krytyczną. Nie mniej ważne jest również zwiększenie poziomu świadomości społeczeństwa w zakresie cyberbezpieczeństwa za pomocą edukacji i szkoleń.

Celem strategicznym w polityce cyberbezpieczeństwa Polski, Niemiec i Wielkiej Brytanii jest niwelowanie możliwości przeprowadzenia cyberataków przez aktorów państwowych i niepaństwowych oraz klasycznych zagrożeń o charakterze kryminalnym[944]. Niemcy niewątpliwie należą do państw, które poważnie traktują zagrożenia cybernetyczne. W RFN opracowano nie tylko dokumenty o charakterze polityczno-programowym, jak *Strategia cyberbezpieczeństwa dla Niemiec* z 2011 r., przyjęto również ustawę, która porządkuje kompetencje organów i systematyzuje proces zapewniania bezpieczeństwa IT.

W niewielu państwach funkcjonuje podobne kompleksowe rozwiązanie prawne w omawianej dziedzinie. Warto dodać, że RFN stara się, aby przyjmowane rozwiązania pozostawały w zgodzie z wytycznymi międzynarodowymi. Pozytywną cechą systemu stworzonego przez Niemcy jest wysoki stopień włączenia w tworzenie

bezpieczeństwa cybernetycznego prywatnych operatorów infrastruktury krytycznej. Są oni nie tylko wykonawcami licznych obowiązków ustawowych, ale także partnerem m.in. w ramach Narodowej Rady Cyberbezpieczeństwa. Na mocy ustawy z 2015 r. biznes może również wprowadzać rozwiązania w typie samoregulacji.

W odniesieniu do istniejącej siatki organów i instytucji zajmujących się bezpieczeństwem cybernetycznym należy stwierdzić, że słowem-kluczem jest „koordynacja". Federalny Urząd Bezpieczeństwa Teleinformatycznego, który funkcjonuje w ramach Ministerstwa Spraw Wewnętrznych, oraz nadzorowane przez niego Narodowe Centrum Przeciwdziałania Cyberzagrożeniom, spełniają funkcję integrującą informacje i kompetencje z różnych obszarów działalności federacji. Co ważne – istnieje platforma współpracy między organami cywilnymi i wojskowymi. Specyficzną cechą niemieckich rozwiązań jest powierzenie BSI kontroli nad sposobem wdrożenia szczegółowych procedur ochronnych w tych działach infrastruktury krytycznej, które decydują o sposobie funkcjonowania społeczeństwa. Moim zdaniem jest to efektywne rozwiązanie zapobiegające dublowaniu kompetencji oraz pułapce braku adresata ważnej informacji.

Niemieckie rozwiązania powodują, że system bezpieczeństwa cybernetycznego koncentruje się na ochronie infrastruktury krytycznej, elementach technologii informatycznych i komunikacyjnych oddziałujących na sposób funkcjonowania społeczeństwa oraz Internet. Za najpoważniejsze zagrożenie uznano cyberataki, cyberszpiegostwo oraz sabotaż. Na wypadek wojny w cyberprzestrzeni strategia pokazuje, że omawiany aspekt nie jest pomijany, choć wciąż wydaje się, że zdolności te traktowane są defensywnie lub jako instrument wspierający działania regularnego wojska, np. podczas zagranicznych misji i operacji.

W Polsce uprawnienia dotyczące cyberbezpieczeństwa mogą być realizowane przez Ministra Obrony Narodowej, Szefa Agencji Bezpieczeństwa Wewnętrznego, Ministra Spraw Wewnętrznych i Administracji, policję, Rządowe Centrum Bezpieczeństwa, Ministra Cyfryzacji. Cyberbezpieczeństwem zajmują się także zespoły CSIRT utworzone przez operatorów telekomunikacyjnych, banki, przedsiębiorstwa energetyczne oraz środowiska naukowo-badawcze.

Wymienione podmioty realizują zadania w zakresie cyberbezpieczeństwa w sferze cywilnej, zwalczania cyberprzestępczości, zapobiegania zdarzeniom terrorystycznym i obrony narodowej.

Przy dużej liczbie podmiotów bezpieczeństwa i porządku publicznego zauważalny jest brak pełnej koordynacji w realizacji przypisanych im kompetencji, które często się nakładają. Szczególnie dokuczliwe w sprawnym funkcjonowaniu tego podsystemu jest powielanie kompetencji kierowniczych, które powinny zostać wyraźnie określone przez regulacje prawne. Te niedociągnięcia dotyczą kompetencji organów władzy publicznej szczebla zarówno centralnego, jak i terenowego. Często kompetencje organów władzy publicznej są niedookreślone lub określone zbyt ogólnikowo[945].

Konieczne jest zatem opracowanie odpowiednich przepisów prawnych gwarantujących zintegrowane, kompleksowe i uporządkowane działania kształtujących pożądaną strukturę organizacyjną, kompetencje służb, zasady koordynacji działania, siły i środki, łączność, zasady finansowania oraz obszary edukacji służb i społeczeństwa. Powinny one także uwzględniać nowe zjawiska przestępcze i nowe narzędzia jej zwalczania.

Przede wszystkim zaś powinny precyzyjnie określać odpowiedzialność poszczególnych instytucji, zasady i procedury koordynowanych przez nich zadań oraz zasady odpowiedzialności. Wydaje się, że w poszczególnych obszarach bezpieczeństwa i porządku publicznego niezbędne jest wyznaczenie liderów, instytucji specjalizujących się w gromadzeniu wiedzy (teoretycznej i praktycznej) z danego zakresu oraz koordynacji działań wszystkich elementów podsystemu obronno-ochronnego. Najlepszym tego przykładem jest zwalczanie przestępczości zorganizowanej, z precyzyjnym określeniem wiodącej roli w realizacji tego zadania. Zdarzają się obszary przestępczości, którymi zainteresowane są prawie wszystkie podmioty, np. terroryzm, nielegalny obrót bronią i amunicją, przestępstwa korupcyjne, przestępczość finansowa, narkotyki[946].

Występująca w Polsce duża liczba podmiotów, a więc rozproszenie kompetencyjne utrudnia kompleksowe rozpoznanie i identyfikację

tego zagrożenia oraz efektywne dysponowanie siłami i środkami w celu przeciwdziałania tego typu przestępczości. Brak jednolitego sposobu rozliczania, ewidencjonowania i porównywania osiąganych wyników w kontekście nakładania się właściwości poszczególnych służb i podmiotów powoduje brak możliwości obiektywnej i porównywalnej oceny ich skuteczności[947].

Należałoby ujednolicić uprawnienia funkcjonariuszy różnych służb, procedury ich działania oraz pragmatyki służbowe. W rezultacie powinna być osiągnięta sytuacja pozwalająca efektywnie dysponować posiadanym zasobem osobowym służb specjalnych, przy założeniu wymienności personelu między służbami i w procesie współdziałania. Na tym tle należy rozważyć propozycję uwolnienia służb specjalnych od obowiązków procesowych (powinny zostać przejęte przez CBŚ) i ograniczyć ich aktywność tylko do śledztw proaktywnych, tj. takich, które zmierzają do uprawdopodobnienia faktu popełnienia przestępstwa.

Moje zastrzeżenia budzi przede wszystkim dualizm regulacji w zakresie przyjętej właściwości odnośnie do konkretnych systemów i usług teleinformatycznych. Nieuwzględnienie zasad właściwości organów wynikających z ustawy o zarządzaniu kryzysowym doprowadzi do sytuacji, w której kwalifikacji tych samych usług dokonywać będą różne podmioty. W przypadku uznania w obu ustawowych reżimach właściwości przez różne organy w odniesieniu do tego samego systemu teleinformatycznego dojdzie do zakłócenia w systemie zapewniania bezpieczeństwa tych systemów.

Kolejną sprawą są bardzo szerokie uprawnienia CSIRT w zakresie możliwości żądania od operatorów telekomunikacyjnych udostępnienia informacji dotyczących działalności oraz przyjętych rozwiązań organizacyjno-technicznych. Wprowadzenie takich rozwiązań, w szczególności z pominięciem analizy ryzyka i bez uwzględnienia zasady adekwatności stosowanych zabezpieczeń do zidentyfikowanych ryzyk, może w istotnym zakresie ograniczać swobodę działalności gospodarczej, a jednocześnie obniżać efektywność prowadzonych działań w obszarze cyberbezpieczeństwa.

Brak jest również jednoznacznego i niebudzącego wątpliwości określenia odpowiedzialności za obsługę incydentu poważnego. Z

jednej strony odpowiedzialność za obsługę incydentu spoczywa na operatorze, z drugiej – ustawa przewiduje wprost uprawnienia CSIRT w zakresie obsługi incydentów poważnych, nie wskazując przy tym zasad podejmowania decyzji przez CSIRT w zakresie incydentów, przyznając CSIRT pewne uprawnienia „władcze" wobec operatora. Tym samym CSIRT miałby możliwość ingerencji w działalność jednostkowego operatora z pominięciem jakiejkolwiek odpowiedzialności za czynności podejmowane wobec niego.

Istnienie punktu zgłoszeń incydentów na poziomie krajowym, do którego można zgłaszać incydenty, do którego obowiązków należałoby przekierowanie incydentu według właściwości, byłoby znacznie efektywniejsze niż zaproponowany dualistyczny, dość skomplikowany model zgłaszania poszczególnych kategorii incydentów w Polsce. Warto w tym kontekście zauważyć, że liczba organów, do których przedsiębiorca powinien zgłaszać incydenty, znacząco wzrasta wraz ze stopniowym wprowadzaniem NIS. Takie obowiązki istniały już w zakresie zgłoszeń do: UKE, GIODO, ministra ds. informatyzacji. Od daty wejścia w życie dyrektywy NIS obowiązek taki został wprowadzony wobec CSIRT NASK (odnośnie do incydentów istotnych przy usługach cyfrowych) oraz odpowiedniego CSIRT (w zakresie incydentów poważnych przy usługach kluczowych.

Warto przypomnieć, że pierwsza strategia cyberbezpieczeństwa Wielkiej Brytanii zawierała głównie ogólnikowe stwierdzenia wskazujące na rosnące zagrożenia związane z działalnością hakerów, akcentowała konieczność współpracy sektorów publicznego i prywatnego oraz międzynarodowej kooperacji. Dużo miejsca poświęcono na opisy zagrożeń i sposobu działań hakerów, ale zabrakło podania konkretnych rozwiązań danych problemów, a także wyznaczenia długoterminowych celów. Jedynym rzeczywistym osiągnięciem obu strategii było powołanie Biura Cyberbezpieczeństwa i Centrum Operacji Cybernetycznych. Wobec tych dwóch instytucji eksperci zgłosili jednak wiele zastrzeżeń. Wskazano, że nie określono ich budżetu, miejsca w brytyjskim systemie legislacyjnym, nie odpowiedziano na pytanie, czy mogą one wpływać na uchylenie umów zawartych przez rząd, które narażają na szwank cyberbezpieczeństwo państwa. Większość specjalistów negatywnie oceniało strategie,

wskazując, że stworzyły one kolejne dwa ciała odpowiedzialne za cyberprzestrzeń, które zamiast wzmocnić efektywność działań, przyczynią się do zwiększenia biurokracji. Należy jednak pamiętać, że opracowana strategia w cyberprzestrzeni była pierwszą w dziejach Wielkiej Brytanii i jedną z pierwszych na świecie. Miała wyznaczać główne trendy w dziedzinie bezpieczeństwa cybernetycznego, a nie proponować konkretne rozwiązania.

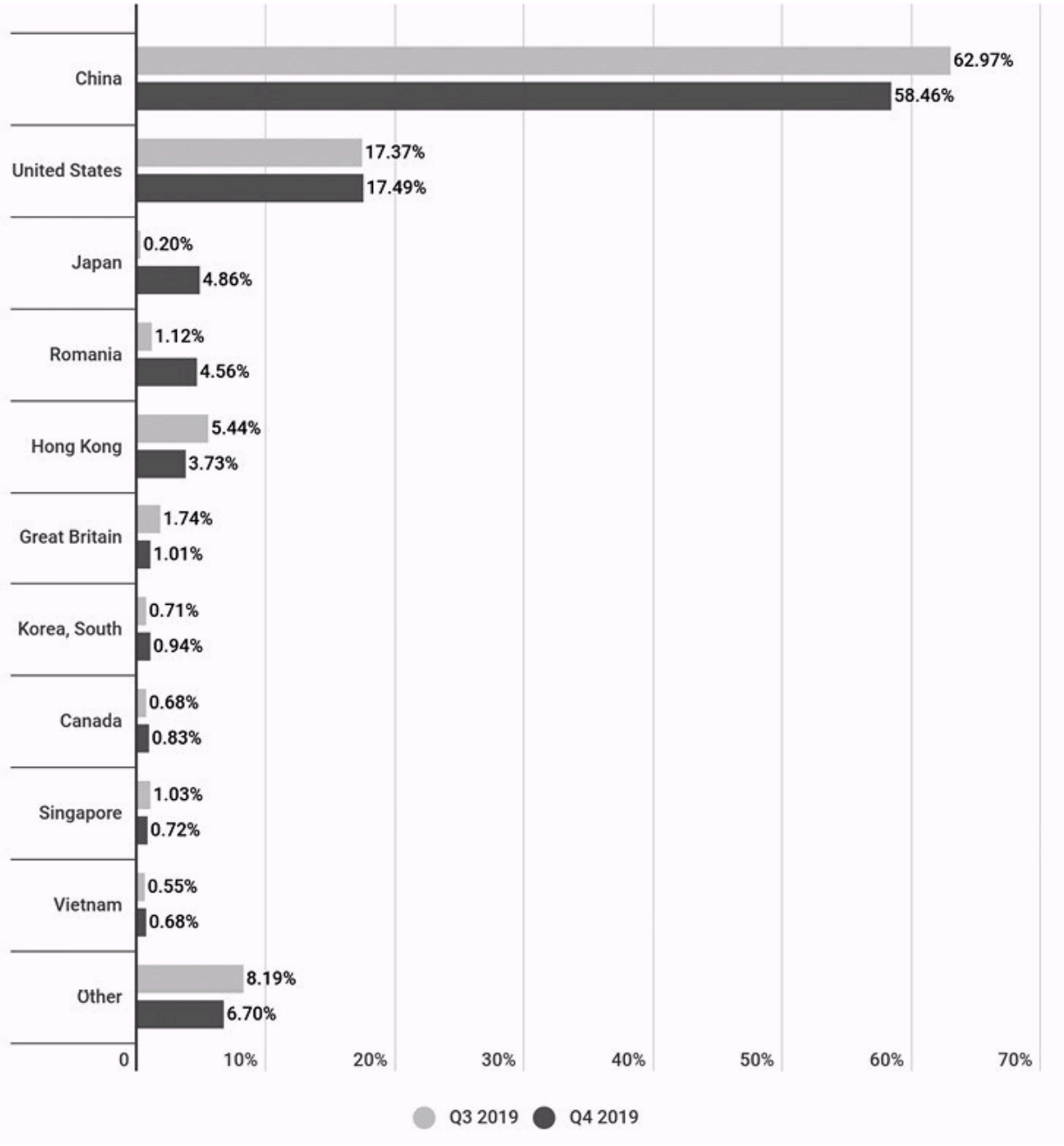
To potwierdza, że polityka Wielkiej Brytanii, instrumenty prawne oraz ostatnia strategia z 2016 r. w zakresie ochrony cyberprzestrzeni stawiają na prewencję będącą właściwym środkiem ochronnym. To sprawia, że Wielka Brytania stała się ważnym graczem (supermocarstwem) w cyberprzestrzeni Europy i świata plasującym się obecnie na drugiej pozycji.

Ewolucja systemu bezpieczeństwa cybernetycznego we Francji, którą zapoczątkowała opracowana w 2008 r. *Biała Księga,* określająca podstawowe cele i założenia polityczne w obszarze cyberbezpieczeństwa, doprowadziła do uporządkowania organizacyjnego i legislacyjnego. Za najważniejszy element procesu tworzenia spójnego systemu zapobiegania i przeciwdziałania zagrożeniom w cyberprzestrzeni należy uznać utworzenie w 2009 r. Narodowej Agencji Bezpieczeństwa Systemów Informatycznych.

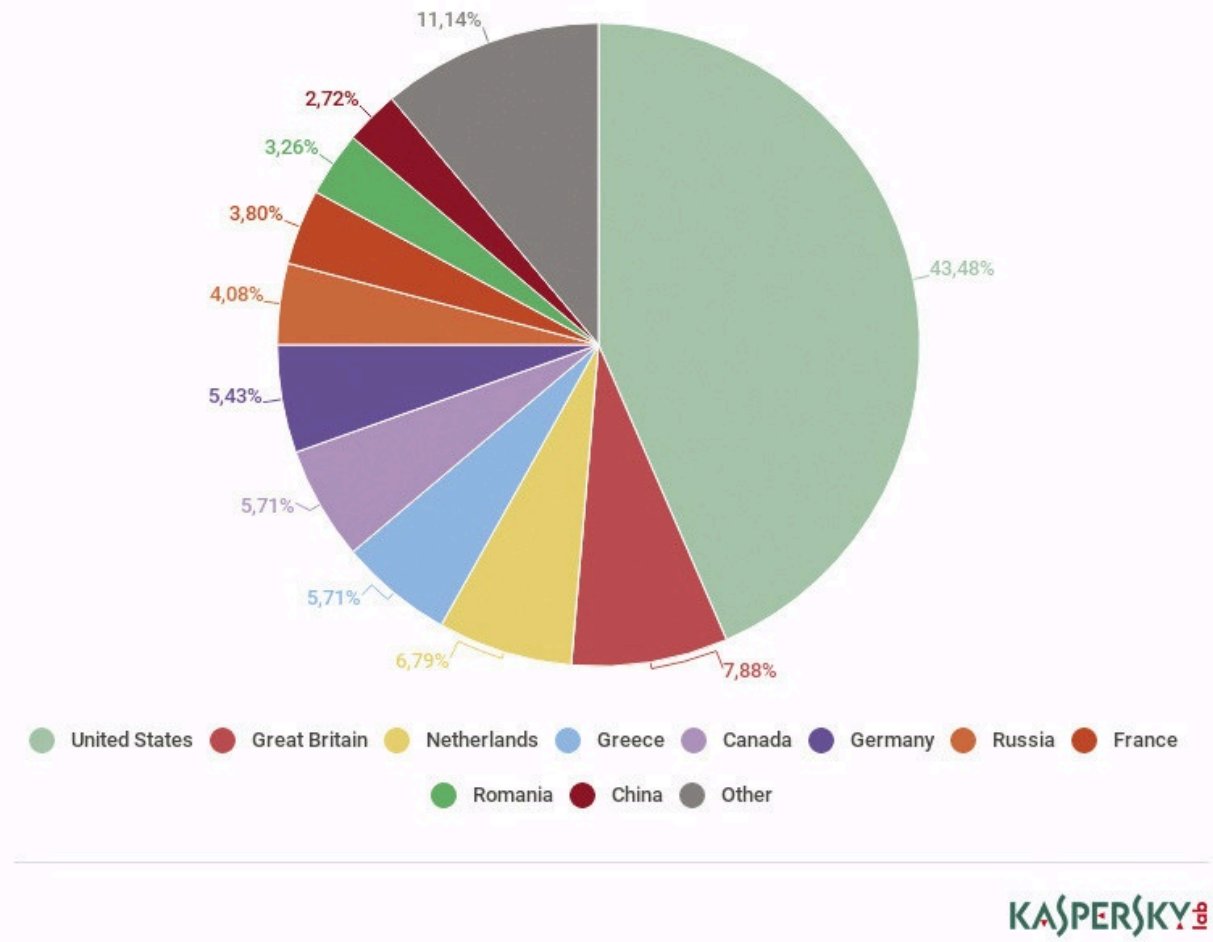
Republika Francuska jest jedynym państwem Unii Europejskiej, której celem polityki bezpieczeństwa cybernetycznego jest zarówno rozwój zdolności o charakterze ofensywnym pozwalających na wsparcie operacji wojskowych, jak i podkreślenie znaczenia gospodarczego wymiaru cyberbezpieczeństwa oraz potencjalnych skutków, jakie mógłby wywołać ewentualny atak informatyczny na systemy wykorzystywane przez najważniejsze przedsiębiorstwa. Takie ujęcie powoduje, że podsystem militarny ochrony cybernetycznej funkcjonuje samodzielnie, a w jego ramach prowadzone są działania o charakterze defensywnym ukierunkowane na ochronę wojskowej infrastruktury informatycznej oraz ofensywnym, a ich zasadniczym celem jest zapewnienie tzw. suwerenności informacyjnej Francji. Warto zauważyć, że potrzeby Francji dotyczące stworzenia skutecznych instrumentów przeciwdziałania zagrożeniom cybernetycznym i reagowania na nie są większe niż pozostałych

państw europejskich (z wyjątkiem Wielkiej Brytanii) z uwagi na posiadanie technologii pozwalających na wykorzystywanie energii nuklearnej w wymiarze cywilnym i wojskowym.

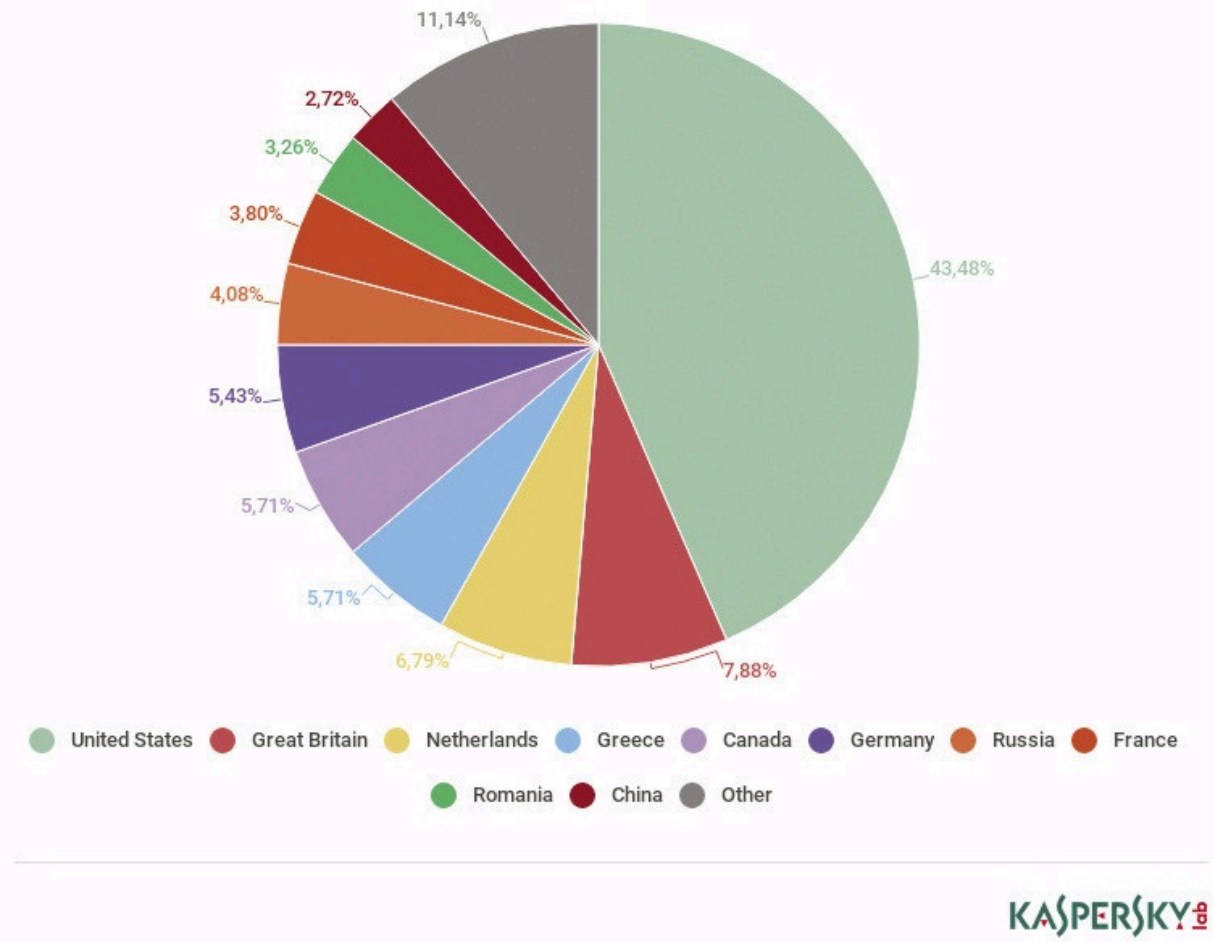
Biorąc pod uwagę kształt ustawowych kompetencji ANSSI, należy uznać, że mają one charakter wyłącznie defensywny. Do najważniejszych z nich zalicza się opracowywanie środków ochrony systemów informatycznych i tworzenie mechanizmów wykrywania zagrożeń w systemach i sieciach. Agencja nie dysponuje jednak instrumentami ofensywnymi pozwalającymi na aktywne zwalczanie incydentów mogących negatywnie wpływać na bezpieczeństwo systemów najistotniejszych – z punktu widzenia funkcjonowania organów państwowych czy operatorów – dla infrastruktury krytycznej.



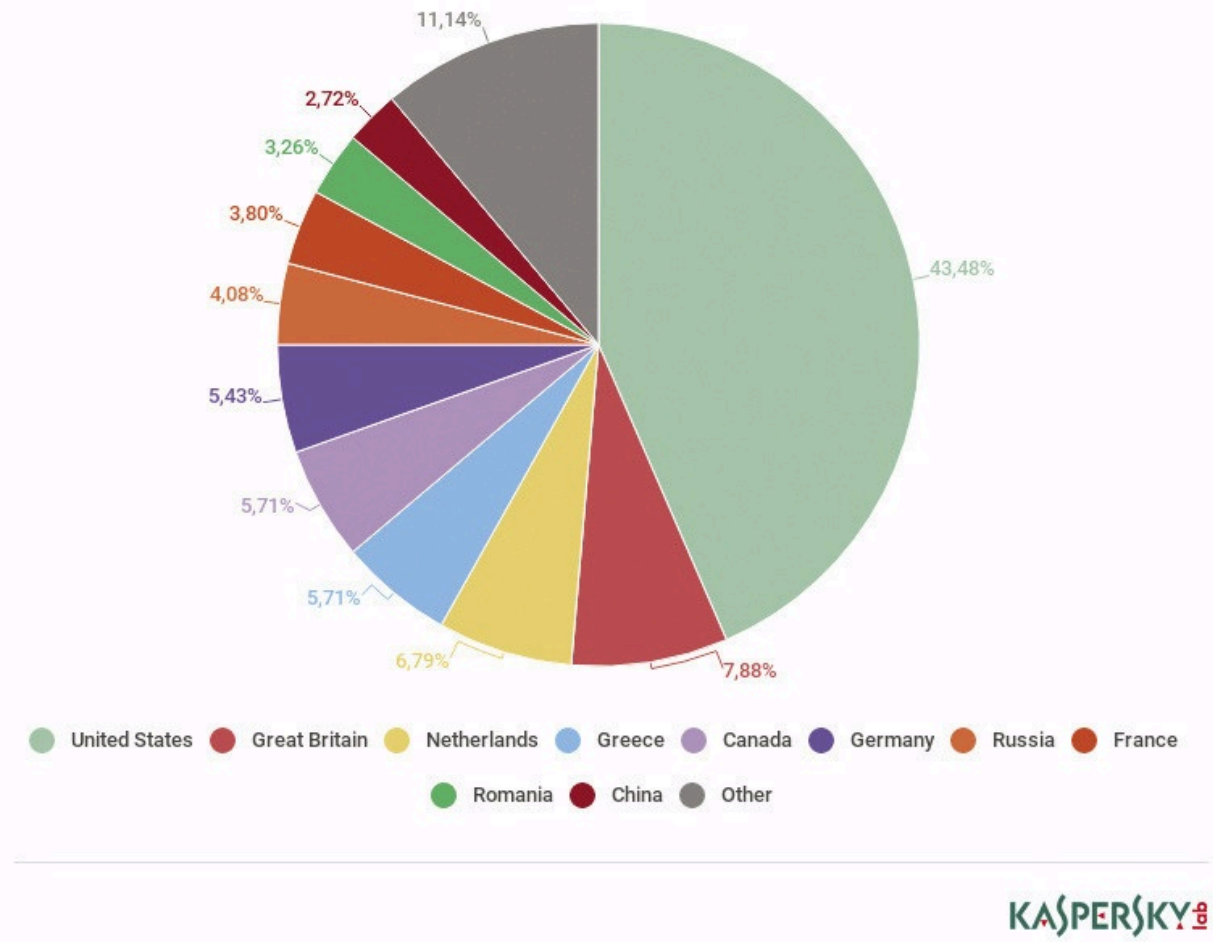
RYSUNEK 6.12 Rozkład ataków DDoS według państw w 2019 r.
Źródło: Raport: http://kaspersky.pl za 2019 r. (dostęp: 21.02.2020).



RYSUNEK 6.13 Rozkład największych graczy w cyberprzestrzeni w 2018 r.
Źródło: Raport: http://kaspersky.pl za 2018 r. (dostęp: 18.03.2019).



RYSUNEK 6.14 Rozkład największych graczy w cyberprzestrzeni w 2019 r.
Źródło: Raport: http://kaspersky.pl za 2019 r. (dostęp: 21.02.2020).



RYSUNEK 6.15 Rozkład liderów ataków w cyberprzestrzeni w 2020 r.
Źródło: www.Kaspersky.pl (dostęp: 30.07.2020).

Przedstawione na *rysunkach 13–16* wykresy potwierdzają, że przyjęta przez Wielką Brytanię *Strategia ochrony cyberprzestrzeni* przyniosła najlepsze efekty w Europie, co daje jej drugie miejsce na świecie. Jeżeli chodzi o region UE, ważnym graczem w tej polityce są Francja i RFN. Chociaż Chiny i Rosja nie są podmiotami badawczymi tej analizy, należy o nich wspomnieć, ponieważ odgrywają istotną rolę w cyberprzestrzeni, będąc jej najważniejszymi graczami, wywierając tym samym wpływ na zmiany w strategii i polityce zarówno UE, jak i poszczególnych państw członkowskich.

7

SKUTKI I PERSPEKTYWY ROZWOJU STRATEGII I POLITYKI CYBERBEZPIECZEŃSTWA UNII EUROPEJSKIEJ

Zapewnienie bezpieczeństwa od wieków stanowi istotną funkcję państwa. Można wysunąć twierdzenie, że elementem wpływającym na ogólny poziom bezpieczeństwa obywateli w państwie jest odpowiedzialna administracja. Nadużycie uprawnień dyskrecjonalnych, niekiedy pozornie prowadzące do ukazania sprawności działania tych organów, powoduje naruszenie zasady praworządności i proporcjonalności. Brak zaufania obywateli wobec tych, którzy działają w imieniu państwa, tworzy atmosferę zagrożenia bezpieczeństwa publicznego i jednostek, a w konsekwencji bywa też pretekstem do zbiorowego nieposłuszeństwa.

W pierwszej części tego rozdziału zostaną przedstawione skutki prowadzonej polityki i strategii Unii Europejskiej w obszarze ochrony cyberprzestrzeni, które następnie zostaną poddane analizie w związku z wdrożeniem wspólnych procedur i harmonizacji zasad prewencji oraz zwalczania cyberterroryzmu na szczeblu europejskim opartych na standardach międzynarodowych.

W drugiej części rozdziału zostaną zaprezentowane scenariusze rozwoju polityki i strategii ochrony cyberprzestrzeni Unii Europejskiej. O rozwoju polityki będą decydowały czynniki wewnętrzne oraz

zewnętrzne, zwłaszcza wzrost gospodarczy w UE, integracja społeczeństwa z napływającą ludnością w państwach członkowskich, szybkość harmonizacji przepisów prawa unijnego. W zależności od tego, które ugrupowania polityczne znajdą się u władzy, będziemy mieć do czynienia albo ze wzrostem harmonizacji prawa, albo z eskalacją wzajemnie napędzających się ekstremizmów i będącego ich owocem terroryzmu, podczas gdy harmonizacja prawa zatrzyma się na dotychczasowym etapie.

Biorąc pod uwagę wymienione czynniki, należy rozważyć trzy scenariusze rozwoju polityki i strategii ochrony cyberprzestrzeni Unii Europejskiej – scenariusz najbardziej oddający stan bieżącej sytuacji, scenariusz najbardziej pożądanej sytuacji oraz scenariusz najbardziej prawdopodobnej sytuacji.

7.1
SKUTKI POLITYKI I STRATEGII CYBERBEZPIECZEŃSTWA UNII EUROPEJSKIEJ

W perspektywie europejskiej wymiar bezpieczeństwa cybernetycznego jest obecnie jednym z najważniejszych priorytetów politycznych Unii Europejskiej, przy czym jego elementy można znaleźć w ramach innych polityk UE[948]. Dla wielu państw wyzwaniem jest także zdefiniowanie polityki cyberbezpieczeństwa będącej złożonym i wielowarstwowym zjawiskiem, która w tym kontekście jest wyraźnie powiązana z innymi politykami. Ponadto przez wdrażanie wielu tematów, wymagań definicyjnych, klasyfikacji, standardów do debaty publicznej oraz certyfikacji i innych procedur UE wpływa i kształtuje politykę cyberbezpieczeństwa państw członkowskich. Istotne są także mniej techniczne tematy, które obejmują: kształtowanie świadomości społecznej w zakresie cyberzagrożeń, budowanie umiejętności i wiedzy przez edukację i wymianę informacji.

Jako regionalny sojusz gospodarczy i polityczny, Unia dąży do realizacji wspólnych interesów 27 państw członkowskich. Fundamentem jej polityki jest rozwój oraz stabilne funkcjonowanie

jednolitego rynku, czyli swobodny przepływ towarów, usług, kapitału i ludzi, określany również jako rynek wewnętrzny. Pojawia się jednak poważny problem, którym jest możliwość wystąpienia paraliżu funkcjonowania jednolitego rynku, czego przykładem były zdarzenia występujące podczas ataków szkodliwych programów, jak WannaCry czy NotPetya w 2017 r., które doprowadziły do zakłóceń funkcjonowania podmiotów międzynarodowych[949].

Należy podkreślić, że w przypadku państw europejskich terroryzm, a tym samym również cyberterroryzm miał początkowo przede wszystkim charakter wewnętrzny. To spowodowało dwojakiego rodzaju następstwa. Państwa uznawały i w dużej mierze nadal uznają, że przeciwdziałanie terroryzmowi jest obowiązkiem, który należy do ich wyłącznej kompetencji. Współpracę międzynarodową w tym zakresie postrzegają jako konieczną, ale stanowiącą jedynie uzupełnienie i poszerzanie zdolności do walki z terroryzmem[950].

Z zaprezentowanych rozważań wynika, że bezpieczeństwo jest wartością, ale też dynamicznym procesem podlegającym ewolucji w warunkach zmiany rzeczywistości społecznej. Zagrożenia stwarzają najczęściej państwa lub podmioty niepaństwowe o stwierdzonych wrogich zamiarach wobec innych państw bądź organizacji, dysponujące środkami ich realizacji. Zagrożenia w sferze teleinformatycznej są coraz trudniejsze do identyfikacji, dążąc do dezorganizacji kluczowych systemów informacyjnych instytucji rządowych, elementów infrastruktury krytycznej, w tym baz danych. Czynnikami sprzyjającymi powstawaniu tego typu zagrożeń są niskie koszty przygotowania operacji i ogromna skala zniszczeń. Cechą charakterystyczną tych działań jest globalny ich zasięg. Walka informacyjna i wojna informacyjna nie są zjawiskiem nowym. Innowacyjne są tylko narzędzia gromadzenia, przetwarzania i przesyłania informacji, a także niespotykanie szybko rosnąca wartość informacji dla osiągnięcia przewagi militarnej, politycznej, ekonomicznej czy informacyjnej.

Zagrożenia bezpieczeństwa społeczeństwa informacyjnego są realne, obecne w codziennej rzeczywistości życia podmiotu, zatem rozpoznanie, osiągnięcie, utrzymanie i doskonalenie bezpieczeństwa informacyjnego staje się konieczne do zapewnienia przewagi konkurencyjnej organizacji, płynności finansowej, rentowności, pozostawania w zgodzie z literą prawa.

Działalność cyberterrorystów w sieci jest dużym problemem, gdyż ich poczynania są ukryte. Z uwagi na łatwość maskowania tożsamości można mówić o relatywnej anonimowości atakujących, którzy bez obaw, że zostaną wykryci, przeprowadzają za pomocą sieci wrogie działania. Wynika stąd kolejny problem – skala potencjalnych strat, zarówno pod względem finansowym, jak i bezpieczeństwa, jest trudna do oszacowania[951].

Należy też stwierdzić, że polityka cyberbezpieczeństwa UE nie jest tylko odpowiedzią, ale także reakcją powstałą na zaistniałe zagrożenie, stanowi ochronę wspólnego dobra[952]. Dzisiaj niemal każda nielegalna działalność ma swoje odbicie w Internecie. Globalny charakter Internetu przyspieszył komunikację i umożliwił przeniesienie większości form aktywności człowieka do sieci, także i tych negatywnych. Coraz powszechniej mówi się o cyberprzestrzeni jako nowej przestrzeni społecznej, w której występują te same problemy co w świecie rzeczywistym. Cyberprzestępczość jest zatem nowoczesną odmianą przestępczości, wykorzystującą możliwości technik cyfrowych i środowiska sieci komputerowych.

Przyczyną powstania polityki cyberbezpieczeństwa był również brak istnienia odpowiednich mechanizmów i regulacji w tym zakresie, w związku z czym mamy do czynienia z procesem instytucjonalizacji. Cyberprzestępczość różni się od klasycznej przestępczości przede wszystkim działaniem w środowisku związanym z technologią komputerową i wykorzystanie sieci komputerowych do ich popełniania[953]. Nową, bardzo niebezpieczną zmianę w cyberterroryzmie wyznacza pojawienie się tzw. najemników. To coraz częstsza tendencja wykorzystywania zaawansowanych technologii w przestępczych działaniach komputerowych[954].

Coraz częściej organizacje ekstremistyczne (głównie islamskie) budują sieci hakerskie w celu wsparcia swoich działań i przeprowadzania ofensywnych ataków. Można wyróżnić trzy poziomy zagrożenia związanego z cyberterroryzmem[955]. Pierwszym z nich jest tzw. *simple-unstructured*, który polega na dokonaniu przez cyberterrorystów prostych włamań do indywidualnych systemów informacyjnych za pomocą narzędzi internetowych skonstruowanych przez inną osobę. Drugim poziomem zagrożenia jest tzw. *advanced-structured*. W tym przypadku cyberterroryści dokonują bardziej

skomplikowanych ataków przeciw złożonym sieciom komputerowym i systemom. Posiadają możliwość tworzenia lub modyfikacji własnych narzędzi, które służą do atakowania w cyberprzestrzeni, mają zdolność analizy celów, które będą przedmiotem ataku, a także dowodzenia, kontroli i uczenia się nowych metod atakowania. Ostatnim, najpoważniejszym poziomem zagrożenia jest tzw. *complex-coordinated*. Cyberterroryści dokonują tu skoordynowanych ataków mających na celu totalną destrukcję zintegrowanego systemu obronnego, mają możliwość tworzenia skomplikowanych narzędzi, które służą do niszczenia celów w cyberprzestrzeni a także analizę celów będących przedmiotem ataku. Mogą dowodzić, kontrolować oraz samodoskonalić się.

Analiza literatury przedmiotu dotycząca zagrożeń i metod przeciwdziałania zagrożeniom oraz obserwacje działań państw i różnego rodzaju organizacji wskazują, że proces ten, poza działaniami specjalistycznymi, powinien być wspierany metodami stosowanymi w obszarze bezpieczeństwa informacji oraz systemów teleinformatycznych i telekomunikacyjnych, zarówno publicznych, jak i mających zastosowania specjalne w obszarze bezpieczeństwa państwa i zarządzania kryzysowego.

Uogólniając prezentowane treści, można sprecyzować kilka wniosków. Po pierwsze, cyberterroryzm jest szczególnym zagrożeniem cywilizacji, społeczeństwa informacyjnego, bezpieczeństwa narodowego i obywateli, które wymaga przeciwdziałania i zdecydowanego zwalczania. W wyniku przyjęcia 14 lutego 2013 r. przez Komisję Europejską wraz z Wysokim Przedstawicielem Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa komunikatu w sprawie europejskiej strategii bezpieczeństwa cybernetycznego *Otwarta, bezpieczna i chroniona cyberprzestrzeń*[956] rozpoczęto modernizację polityki i strategii w obszarze cyberbezpieczeństwa UE. Kolejnym działaniem było przyjęcie 6 lipca 2016 r. dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium UE, która zobowiązała wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu zdolności krajowych w dziedzinie cyberbezpieczeństwa przez ustanowienie organów właściwych oraz pojedynczego punktu kontaktowego ds. cyberbezpieczeństwa, powołanie zespołów

reagowania na incydenty komputerowe (CSIRT) oraz przyjęcia krajowych strategii w zakresie cyberbezpieczeństwa.

Po drugie, w nowym dokumencie po raz pierwszy wyrażono potrzebę „utrzymania i rozwoju przez UE podstawowych zdolności do zapewnienia bezpieczeństwa gospodarki cyfrowej, społeczeństwa i demokracji", a celem polityki UE stało się zmniejszenie fragmentaryzacji rynku oraz rozwinięcie zdolności gospodarczych i poprawa działań wobec incydentów cybernetycznych. Konkretne działania polityczne nastąpiły w 2017 r. Jednym z zadań polityki UE w zakresie cyberbezpieczeństwa było wzmocnienie zdolności i współpracy dotyczących bezpieczeństwa cybernetycznego w celu zapewnienia takiego samego poziomu rozwoju we wszystkich państwach członkowskich. We wrześniu 2017 r. Komisja Europejska rozpoczęła przegląd ESB cybernetycznego z 2013 r., wydając dokument roboczy przedstawiający jej ocenę[957], zgodnie z którą strategia ta była tylko częściowo skuteczna z powodu niewystarczających zasobów i ograniczonego zaangażowania kluczowych podmiotów. Ponadto od tamtej pory możliwości i zagrożenia w cyberprzestrzeni znacznie się rozwinęły. Czynniki te uzasadniły więc podjęcie ważnego kroku, tj. odnowienie strategii cyberbezpieczeństwa.

Podstawą reformy były działania przewidziane w ESB cyberbezpieczeństwa oraz główny filar strategii – dyrektywa o bezpieczeństwie sieci i informacji (dyrektywa NIS)[958], która ma na celu zapewnienie sprawnego funkcjonowania europejskiego rynku wewnętrznego. Wymaga ona także, aby wszystkie państwa UE posiadały zdolności w zakresie cyberbezpieczeństwa oraz współpracowały na poziomie strategicznym i operacyjnym. Innym ważnym aktem prawnym jest rozporządzenie w sprawie ochrony danych (GDPR, inaczej RODO)[959].

Po trzecie, w wyniku obecności ogromnej skali cyberzagrożeń zaczęły pojawiać się głosy, że UE nie spełnia oczekiwań w dziedzinie cyberobrony[960]. Ponadto państwa członkowskie wciąż rozwijały rozbieżne strategie cyberbezpieczeństwa oraz wyrażały odmienne poglądy na temat tego, jak podmioty państwowe oraz instytucje UE powinny przyczyniać się do odporności cybernetycznej na szczeblu europejskim. W rezultacie każdy obszar europejskiej strategii bezpieczeństwa cybernetycznego wydanej w 2013 r. znajdował się na

innym etapie rozwoju. Dyrektywa 2016/1148 (NIS) jest pierwszym aktem prawa UE w zakresie cyberbezpieczeństwa wprowadzającym regulacje międzysektorowe. Czas na implementację dyrektywy do porządków prawnych państw członkowskich upłynął 9 maja 2018 r. Tekst dyrektywy koncentruje się wokół trzech filarów:

- instytucji, jakie powinny powstać we wszystkich państwach członkowskich;
- współpracy na poziomie europejskim;
- zobowiązań w zakresie bezpieczeństwa sieci i informacji.

Po czwarte, najnowszym posunięciem w polityce cyberbezpieczeństwa jest wydanie w 2020 r. *Białej Księgi* dotyczącej sztucznej inteligencji (AI) i cyfryzacji, która ma stanowić klucz do zwalczenia cyberterroryzmu i osiągnięcia ładu klimatycznego przez doskonalenie AI[961]. To konieczny element pozwalający na utrzymanie jednolitego rynku UE za pomocą badań naukowych, innowacji i wdrożeń do grudnia 2020 r., skoordynowanego planu działań w ramach programów *Cyfrowa Europa* oraz *Horyzont Europa* na lata 2021–2027.

Po piąte, cyberterroryzm i zagrożenia z nim związane mają charakter asymetryczny i ponadnarodowy. Przeciwdziałanie zjawisku nie jest zagadnieniem prostym, ponieważ należy prowadzić działania systemowe na wielu płaszczyznach. Istnieje wiele powodów, dla których przeciwdziałanie cyberterroryzmowi napotyka wiele przeszkód. Należy do nich zaliczyć: niepaństwowy charakter, niebezpośredniość ataku, prowadzenie ataku na odległość, możliwość rozłożenia go w czasie, łatwość przeprowadzenia ataku, konieczność nieustannego dopracowywania rozwiązań formalnoprawnych służących przeciwdziałaniu cyberterroryzmowi. Aktów cyberterroryzmu można dokonać stosunkowo niskim kosztem –wystarczy laptop i dostęp do Internetu. Korzystanie przez terrorystów z elektronicznych kanałów porozumiewania się na odległość może dawać wrażenie anonimowości i niemożności ich wykrycia. To mylne przekonanie. Niemal każda działalność w sieci pozostawia po sobie cyfrowy ślad. Służby wywiadowcze państw stale przeprowadzają działania w celu zbierania takich dowodów, wykrywania sprawców i zapobiegania atakom.

Cyberterroryzm należy do jednego z zagrożeń hybrydowych państwa, którego celem jest nie tylko spowodowanie bezpośrednich szkód i

wykorzystanie jego słabości, ale także destabilizacja społeczeństwa. Zagrożenie to jest coraz bardziej realne. Terroryści zrozumieli, że przestrzeń wirtualna ma gigantyczny wpływ na opinię publiczną, a treści publikowane w Internecie mogą być dodatkowym narzędziem terroru.

Po szóste, wszystkie omówione akty prawne i dokumenty łączy jednak wspólny mianownik. Jest nim problem w zakreśleniu kompetencji i uprawnień państw co do regulowania przestrzeni wirtualnej. Szczególnym wyzwaniem jest ustalenie granic jurysdykcji państw, zwłaszcza że część z nich podejmuje kroki w celu znacznego rozszerzenia swojego władztwa jurysdykcyjnego. Spór w zakresie jurysdykcji stawia pytanie o prawo właściwe w przypadku popełnienia cyberprzestępstwa, działań terrorystów w przestrzeni wirtualnej czy kwestii związanych z codziennym życiem miliona ludzi – handlem elektronicznym czy granicami wolności słowa.

Organizacje międzynarodowe, tj. UE, RE czy ONZ, podejmują próbę regulowania najbardziej newralgicznych kwestii związanych z działalnością człowieka w cyberprzestrzeni. Organizacją o największym zasięgu jest ONZ, która działając za pomocą swoich wyspecjalizowanych agencji, proponuje rozwiązania w zakresie cyberprzestępczości (UNODC) czy handlu elektronicznego (UNICITRAL). Podmiotem, który może w przyszłości odegrać szczególnie ważną rolę, jest Forum Zarządzania Internetem będące nowym modelem tworzenia wspólnej polityki na poziomie międzynarodowym. Wprawdzie IGF nie może wydawać decyzji merytorycznych, lecz przedstawianie rekomendacji w formie modelu *soft law* może sprawdzić się w odniesieniu do przyszłych wyznań związanych z regulacją cyberprzestrzeni.

Unia Europejska za przykładem Rady Europy musi zdecydowanie przeciwstawić się ogólnoświatowemu trendowi podważania prywatności wszystkich w dążeniu do szybszych i łatwiejszych naruszeń praw w cyberprzestrzeni. Jak pokazały rozmowy w Octopus, wiele światowych organów ścigania poszukuje danych o użytkownikach, a zarówno Unia Europejska, jak i Rada Europy muszą stanowczo twierdzić, że przestrzegają międzynarodowych praw człowieka, zwłaszcza art. 15 konwencji budapeszteńskiej, gdy przekraczają jej granice.

Szczególną uwagę należy zwrócić na pracę regionalnych organizacji międzynarodowych oraz ich wkład w tworzenie cyberprawa. Jednym z pierwszych holistycznych aktów prawnych poruszających problem działalności kryminalnej człowieka w cyberprzestrzeni była *Konwencja Rady Europy o cyberprzestępczości*. Do wskazanej umowy międzynarodowej przystąpiło wiele państw również spoza Rady Europy, a niezliczona liczba państw nowelizowała swoje krajowe kodeksy karne, wprowadzając penalizację cyberprzestępstw, opierając się właśnie na wspomnianym traktacie. Konwencja o cyberprzestępczości zawiera jednak głównie przepisy materialnoprawne, nie poruszając zagadnienia związanego z pracą dochodzeniowo-śledczą i koniecznej współpracy w zakresie kryminalistyki. Regulacjami o szczególnym znaczeniu są również *Protokół dodatkowy do konwencji o cyberprzestępczości* dotyczący kryminalizacji działań o charakterze rasistowskim i ksenofobicznym popełnianych przy użyciu systemów komputerowych oraz *Konwencja Rady Europy o ochronie dzieci przed wykorzystaniem seksualnym i niegodziwym traktowaniem w celach seksualnych*.

Z europejskiego punktu widzenia organizacją międzynarodową o największym oddziaływaniu na prawo państwowe oraz europejską unifikację przepisów jest Unia Europejska. Bez wątpienia jest ona liderem w zakresie przyjętych rozwiązań oraz szczegółowości poruszanych kwestii. Inne organizacje międzynarodowe decydują się na uregulowanie jedynie ściśle określonych kwestii, takich jak handel elektroniczny czy cyberprzestępczość. Unia Europejska podejmuje próbę regulacji niemal każdego aspektu prawa cyberprzestrzeni – przestępczości, handlu, własności intelektualnej, danych osobowych, wolności słowa. Dzięki wprowadzonym normom rynek europejski jest najbardziej spójny, a internauci łatwiej dochodzą swoich praw. Tym, co negatywnie wpływa na kształt i efektywność unijnego prawa, jest ogromna fragmentaryzacja i różnice w implementacji ustawodawstwa UE do krajowych porządków prawnych. Istnieją obszary, w których widoczna jest potrzeba wprowadzenia jednego holistycznego dokumentu zamiast kilkunastu szczegółowych aktów prawnych. Również dyrektywa o handlu elektronicznym, wydana kilkanaście lat temu[962], powinna zostać znowelizowana, aby odpowiadać wyzwaniom współczesnego e-commerce.

Cyberprzestrzeń jako przestrzeń globalna, ponadnarodowa i transgraniczna nie ogranicza się wyłącznie do rozwiązań regionalnych. Wyspecjalizowane jednostki, takie jak NATO, coraz wyraźniej zaznaczają problem cyberagresji między państwami, które mogą stanowić element wojny hybrydowej. Obawa ta jest realna. Przytoczone przykłady cyberagresji na Estonię i Gruzję wskazują, że oprócz wojen na lądzie, w wodzie i w powietrzu pojawią się konflikty również w przestrzeni wirtualnej, paraliżując systemy bądź dezinformując przeciwnika. Dlatego też konieczne jest wprowadzenie polityki cyberbezpieczeństwa w krajowych porządkach prawnych. Nie mniej istotna, np. w kontekście nasilającego się terroryzmu oraz walki z Państwem Islamskim, jest konieczność koordynacji i współpracy działań w zakresie walki z cyberprzestępczością i cyberterroryzmem. W takich organizacjach jak Interpol czy Europol wykształcono wyspecjalizowane jednostki, które mają zapobiec, ścigać i zwalczać najpoważniejsze cyberprzestępstwa, czyli cyberterroryzm, pornografię dziecięcą czy pranie brudnych pieniędzy. Tylko skorelowane międzynarodowe działania mogą przynieść oczekiwany skutek. Cyberprzestępcy stają się coraz bardziej pomysłowi, wykorzystują najnowsze techniki i nierzadko drogi, specjalistyczny sprzęt. Efektywna walka z przestępczością wirtualną powinna się zacząć od stałej współpracy, wymiany doświadczeń oraz informowania o zagrożeniach. Niezbędne są również szkolenia organów ścigania, organów sprawiedliwości oraz techników kryminalistycznych w zakresie technik i metod prowadzenia postępowania cyfrowego oraz zbierania i wykorzystania w sądzie dowodów cyfrowych. Instytucją, która może w przyszłości mieć szczególne znaczenie, jest Europejskie Centrum ds. Walki z Cyberprzestępczością powołane do zapobiegania najpoważniejszym przestępstwom popełnianym w cyberprzestrzeni, związanym z przestępczością zorganizowaną, seksualnym wykorzystywaniem dzieci i pornografią dziecięcą oraz ochroną infrastruktury krytycznej Unii Europejskiej i zwalczania ich.

Nie należy również pomijać wkładu organizacji wyspecjalizowanych podejmujących kroki legislacyjne w celu zapewnienia bezpieczeństwa sieci (ENISA) oraz standaryzowania i regulowania rynku telekomunikacyjnego m.in. w zakresie ochrony przed cyberprzestępczością (ITU). Odzwierciedleniem wolnościowego

charakteru cyberprzestrzeni jest organizowanie Światowego Szczytu Społeczeństwa Informacyjnego o elastycznej formule, wskazującego kierunki działań w zakresie budowy społeczeństwa informacyjnego, powszechnego dostępu do informacji oraz Internetu. OECD za pomocą regulacji typu *soft law* podjęła się wytyczenia kierunku zmian legislacyjnych dotyczących podpisu elektronicznego oraz technicznych i prawnych aspektów handlu elektronicznego.

Analiza wybranych dokumentów prowadzi do wniosku, że istniejące rozwiązania traktatowe są fragmentaryczne, a więc niewystarczające. Przyjęcie umowy międzynarodowej jest procesem długotrwałym, poprzedzonym wieloletnimi konsultacjami mającymi na celu wypracowanie konsensusu. Cyberprzestrzeń, jako dynamiczny obszar podlegający szybkim zmianom, jest zawsze krok przed normami prawa pozytywnego. Przestrzeń wirtualna nie może być jednak obszarem, w którym brak jest norm czy chociaż minimalnych standardów. Z tych względów część organizacji międzynarodowych proponuje rozwiązania modelowe, przyjmuje rezolucje i zalecenia, które wskazują kierunki rozwoju prawa cyberprzestrzeni. Wydaje się, że *soft law* odgrywa ogromną rolę w kształtowaniu się norm przestrzeni cyfrowej. Z jednej strony oddolne, nieformalne tworzenie norm odpowiada wolnościowemu charakterowi cyberprzestrzeni, z drugiej – w sposób stosunkowo szybki jest w stanie reagować na nowe wyzwania oraz dynamicznie zmieniającą się sytuację polityczną i technologiczną w globalnym świecie.

W mojej ocenie szczególnie interesujące okazało się porównanie ustawodawstwa poszczególnych państw. Cyberatak na inne państwo może być uznany za naruszenie art. 5 Traktatu Północnoatlantyckiego. Tymczasem porządki prawne niektórych państw, mimo deklarowanych wartości i wolnościowego charakteru przestrzeni wirtualnej, dopuszczają możliwość cyberagresji i rozwiązywania konfliktów „na własnych warunkach", będąc jednostronną próbą usprawiedliwienia ingerencji w przestrzeni wirtualnej obcego państwa. Dlatego też należy przyjąć rozwiązania podobne do rozwiązań wprowadzonych w Estonii, gdzie stworzono cyberarmię złożoną z ochotników, których zadaniem jest obrona cyberprzestrzeni swojego państwa w przypadku wystąpienia ataku.

Konieczne jest zatem stworzenie odpowiednich przepisów prawnych gwarantujących zintegrowane, kompleksowe i uporządkowane działania, kształtujących pożądaną strukturę organizacyjną, kompetencje służb, zasady koordynacji działania, siły i środki, łączność, zasady finansowania oraz obszary edukacji służb i społeczeństwa. Powinny one również uwzględniać nowe zjawiska przestępcze i nowe narzędzia ich zwalczania. Przede wszystkim powinny precyzyjnie określać odpowiedzialność poszczególnych instytucji, zasady i procedury koordynowanych przez nie zadań oraz zasady odpowiedzialności. Wydaje się, że w poszczególnych obszarach bezpieczeństwa i porządku publicznego niezbędne jest wyznaczenie liderów, instytucji specjalizujących się w gromadzeniu wiedzy z danego zakresu oraz koordynacji działań wszystkich elementów podsystemu obronno-ochronnego. Najlepszym tego przykładem jest zwalczanie przestępczości zorganizowanej z dokładnym określeniem wiodącej roli w realizacji tego zadania. Występują obszary przestępczości, którymi zainteresowane są prawie wszystkie podmioty, np. terroryzm, nielegalny obrót bronią i amunicją, przestępstwa korupcyjne, przestępczość finansowa czy narkotyki[963].

We wszystkich państwach UE dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii z dnia 6 lipca 2016 r., zwana dalej dyrektywą NIS, jest wprowadzona szerzej, niż wynika to z jej zapisu. W przypadku Polski uwzględniono dodatkowe sektory, takie jak energetyczny i węglowy, a także związane ze zdrowiem i bakowością.

Sieci oraz systemy i usługi informatyczne odgrywają ważną rolę w społeczeństwie. Skala, częstotliwość oraz wpływ incydentów w zakresie bezpieczeństwa stają się coraz większe i stanowią poważne zagrożenie funkcjonowania działalności gospodarczej i społecznej, w szczególności rynku wewnętrznego. Bezpieczeństwa sieci i systemów informatycznych w Unii różnią się pod względem poziomu ich gotowości, co powoduje niejednolite podejście w ramach UE. Z kolei brak wspólnych wymogów dotyczących operatorów usług kluczowych i dostawców usług cyfrowych uniemożliwiał ustanowienie całościowego i skutecznego mechanizmu współpracy na poziomie Wspólnoty. Skuteczne reagowanie na wyzwania związane z zapewnieniem bezpieczeństwa sieci i systemów

informatycznych wymagało zatem przyjęcia całościowego podejścia na poziomie Unii, obejmującego wymogi dotyczące budowania i planowania wspólnych minimalnych zdolności, wymianę informacji, współpracę oraz wspólne wymogi w zakresie bezpieczeństwa dla operatorów usług kluczowych i dostawców usług cyfrowych.

Normalizacja wymogów w zakresie bezpieczeństwa jest procesem napędzanym przez rynek. W celu zapewnienia harmonizacji przepisów z zakresu ochrony cyberprzestrzeni państwa członkowskie powinny zapewnić wysoki poziom bezpieczeństwa sieci i systemów informatycznych na poziomie Unii dzięki ENISA. W tym celu pomocne mogłoby być opracowanie zharmonizowanych norm, czego należy dokonać zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1025/2012[964].

Pojęcie cyberprzestrzeni w prawie było bardziej kłopotliwe niż klarowne, stwarzając przy tym pewne problemy w jej precyzyjnym interpretowaniu. Dopiero wejście w życie dyrektywy NIS je doprecyzowało[965]. Ponadto problematyka prawna cyberprzestrzeni nie była i nie jest wystarczająco uregulowana w skali globalnej[966]. Wprawdzie w państwach członkowskich Unii Europejskiej są dokumenty w pewnym stopniu regulujące incydenty w cyberprzestrzeni, jednak nie istnieją żadne normy ujmujące prawnie cyberprzestrzeń w skali światowej, których przestrzeganie byłoby egzekwowane. W innych dokumentach tego typu można znaleźć opisane obszary bezpieczeństwa państwa obejmujące problematyką różne podmioty, dziedziny i sektory bezpieczeństwa narodowego, w tym cyberbezpieczeństwo[967]. Wspomniana dyrektywa ma zastosowanie wyłącznie do tych administracji publicznych, które zostały zidentyfikowane jako operatorzy usług kluczowych. Państwa członkowskie pozostają jednak odpowiedzialne za zapewnienie bezpieczeństwa sieci i systemów informatycznych administracji publicznych niewchodzących w zakres stosowania niniejszej dyrektywy.

Producenci sprzętu i twórcy oprogramowania nie są operatorami usług kluczowych ani dostawcami usług cyfrowych, choć ich produkty zwiększają bezpieczeństwo sieci i systemów informatycznych. Odgrywają oni zatem ważną rolę w umożliwianiu operatorom usług kluczowych i dostawcom usług cyfrowych zabezpieczenia ich sieci i systemów informatycznych

W przypadku cyberbezpieczeństwa najpoważniejszym zagrożeniem jest cyberterroryzm definiowany jako „przemyślany politycznie lub niemilitarnie motywowany atak albo groźba ataku na systemy teleinformatyczne w celu sparaliżowania lub poważnego zniszczenia Infrastruktury Krytycznej Państwa oraz zastraszenia i wymuszenia na rządzie lub społeczności daleko idących polityczno-militarnych działań.

Podsumowując rozważania, należy stwierdzić, że obserwowany wzrost poziomu zagrożenia cyberterrorystycznego w państwach Europy Zachodniej, czego przykład stanowią zamachy w Niemczech, Francji, Belgii, Holandii, Wielkiej Brytanii, skutkuje podejmowaniem pewnych kroków i starań zmierzających do zmiany przepisów w celu wzmocnienia możliwości rozpoznawania, przeciwdziałania i zwalczania ewentualnych zagrożeń o charakterze cyberterrorystycznym. Czynią to zarówno poszczególne państwa, jak i gremia oraz organizacje międzynarodowe, których członkiem jest Polska,

Występowanie aktów cyberterroryzmu jest związane zarówno z trychotomią zjawiska cyberprzestępstwa, jak i testowaniem zabezpieczeń rządowych oraz sprawności działania systemów ochronnych. W latach 2013–2019 Polska była najbardziej narażonym państwem w Grupie Wyszehradzkiej na cyberataki pochodzące spoza własnego terytorium. Przełomowym okresem w zakresie cyberzagrożeń był 2014 r., od tego momentu bowiem dostrzegalny jest wzrost liczby cyberincydentów politycznych polegający na penetracji baz danych i wykradaniu z nich poufnych informacji. W przypadku Polski większość incydentów wykorzystuje napięcia społeczne w państwie.

Zmienność metod stosowanych przez cyberterrorystów powoduje, że państwa takie jak Polska muszą posiadać odpowiednie instrumenty służące właściwemu rozpoznawaniu i ocenianiu zagrożeń oraz skutecznemu przeciwdziałaniu ewentualnym zdarzeniom. W przypadku ataku cyberterrorystycznego Polska musi być przygotowana do podjęcia natychmiastowych i adekwatnych środków reagowania, a także usuwania jego skutków. Osiągnięcie tych celów wymaga zapewnienia mechanizmów współpracy wszystkich służb, organów i instytucji zaangażowanych w szeroko rozumiane działania antyterrorystyczne, jak również władz lokalnych, sektora prywatnego oraz całego społeczeństwa.

Wadą polskich rozwiązań jest ich konceptualny charakter oraz pozostawienie ich na etapie wdrażania i nowelizacji. Warto zaznaczyć, że są one zbieżne co do istoty celów strategicznych z założeniami polityki antyterrorystycznej UE. Celem działań administracji państwowej jest zapewnienie akceptowalnego poziomu bezpieczeństwa publicznego w obszarze zwalczania cyberterroryzmu, zwłaszcza krajowej infrastruktury teleinformatycznej, uzyskanie zdolności do zapobiegania zagrożeniom również w cyberprzestrzeni i zwalczania ich oraz zmniejszania skutków potencjalnych incydentów godzących w bezpieczeństwo państwa[968] Podstawową determinantą określającą zasady działania i sposób organizacji systemu bezpieczeństwa publicznego w obszarze walki z cyberterroryzmem jest klasyfikacja podatnych na konsekwencje wrogich działań z wykorzystaniem elementów infrastruktury krytycznej oraz potencjalnych jej zagrożeń. Uzupełnieniem przedsięwzięć ochronnych tych elementów ma być system monitoringu i wczesnego ostrzegania o zagrożeniach[969].

Należy również podkreślić, że ochrona cyberprzestrzeni jest jednym z podstawowych zadań administracji państwowej i podmiotów odpowiedzialnych za tego typu zadania. Powinna stanowić priorytet dla organizacji międzynarodowych i różnego rodzaju kooperacji w skali globalnej i regionalnej. Przykładem mogą być działania administracji Unii Europejskiej, która przypisuje szczególne znaczenie zwalczaniu cyberterroryzmu oraz ochrony cyberprzestrzeni i jej funkcjonowania.

Polityka cyberbezpieczeństwa Unii Europejskiej powinna zmierzać w kierunku zapewnienia bezpieczeństwa systemów informacyjnych, które jest istotą bezpieczeństwa informacyjnego. Bezpieczeństwo informacyjne ze względu na jego znaczenie należy rozpatrywać w obszarach bezpieczeństwa organizacji i instytucji oraz obywatela. Wcześniej o kształcie obiegu informacji decydowała struktura społeczna. Obecnie nie tylko ona ma znaczenie, ponieważ w systemie informacyjnym wywierającym wpływ na społeczeństwo oprócz państwa występują środki masowego przekazu i cyberprzestrzeń.

Formy cyberterroryzmu, rodzaje ataków i metody ich prowadzenia są znane oraz powtarzające się. Przygotowanie na wymaganym poziomie zasobów osobowych i materialnych państwa oraz organizacji umożliwia skuteczną ochronę cyberprzestrzeni. Metody i sposoby zapewnienia bezpieczeństwa informacji i systemów teleinformatycznych organizacji

powinny być stosowane w sposób kompleksowy. Taka praktyka działania wychodzi naprzeciw potrzebom ochrony cyberprzestrzeni.

7.2
PERSPEKTYWY POLITYKI I STRATEGII CYBERBEZPIECZEŃSTWA UNII EUROPEJSKIEJ

Polityka bezpieczeństwa jest jednym z wrażliwych obszarów integracji europejskiej. Świadczy o tym przekonanie wielu decydentów politycznych, że państwo nie posiada suwerenności bez autonomii w zakresie obrony narodowej. Unia Europejska, będąc organizacją międzynarodową, przyczynia się do tworzenia klimatu zrozumienia i współpracy na poziomach regionalnym i globalnym. Polityka ta opiera się obecnie na Traktacie z Lizbony, który wprowadził stanowisko Wysokiego Przedstawiciela Unii ds. Zagranicznych i Polityki Bezpieczeństwa oraz Europejską Służbę Działań Zewnętrznych. Stanowi to istotne narzędzie rozwoju, bez którego UE nie mogłaby wykraczać poza ramy współpracy gospodarczej między państwami członkowskimi ani odgrywać roli czynnika stabilności regionalnej, której oczekują od niej decydenci polityczni i obywatele. Wzrost zagrożenia terrorystycznego, cyberterrorystycznego czy migracji nasila się wraz ze znoszeniem granic. Dla zapewnienia bezpieczeństwa europejskiego konieczna jest więc coraz ściślejsza współpraca między państwami. Dlatego też zwalczanie terroryzmu międzynarodowego i stworzenie odpowiednich mechanizmów współpracy na szczeblu unijnym zostały objęte procesem integracji. Współpraca międzynarodowa w obszarze quasi-militarnym powinna obejmować również działania polityczne, dyplomatyczne i ekonomiczne, aby z odwagą i determinacją rozwiązywać ewentualne sytuacje ucisku i izolacji, które mogą prowokować powstawanie programów terrorystycznych czy cyberterrorystycznych. Obecna polityka cyberbezpieczeństwa Unii Europejskiej powinna zatem zmierzać zarówno do wskazania nowych przyczyn tego zjawiska, jak i stworzenia zintegrowanego systemu

obronnego cyberprzestrzeni na terenie poszczególnych państw i całej UE[970].

Biorąc pod uwagę główne źródła cyberataku w Europie, podobnie jak na całym świecie, są nimi: kryptowaluciarze, botnety, oszustwa bankowe, kradzież informacji komputerowych, ramsonware. Różnią je natomiast szczegółowe dane statystyczne liczby popełnionych przestępstw w poszczególnych regionach, np. w Europie Środkowo-Wschodniej w porównaniu do Ameryki Północnej. Nie różnią się one jednak w sposób znaczący[971].

Scenariusze stanowią zestawienie hipotetycznych zdarzeń opracowanych w celu zwrócenia uwagi na ważne wydarzenia i ich przyczyny. Mają one udzielać odpowiedzi na dwa pytania: w jakiej formie i dlaczego dana hipoteza może się stopniowo spełniać oraz jakie są możliwości zahamowania, zmiany lub przyśpieszenia zjawiska w każdej fazie jego ewolucji (opisanej w scenariuszu). W zasadzie może być to sporządzenie trzech scenariuszy przyszłego stanu społeczeństwa informacyjnego:

- scenariusza najbardziej reprezentatywnego stanu bieżącej sytuacji;
- scenariusza najbardziej pożądanej sytuacji;
- scenariusza najbardziej prawdopodobnej sytuacji.

Faktem niepodważalnym jest duże zróżnicowanie społeczeństw świata, nawet segmentów i grup wewnątrz nich. Są więc też społeczeństwa preinformacyjne, społeczeństwa informacyjne, społeczeństwa we wstępnej fazie informacyjności, a także społeczeństwa postinformacyjne. Te ostatnie to liderzy techniczni, liderzy procesów tworzenia i stosowania wiedzy. Szybkości rozwoju informacyjnego są zróżnicowane, podobnie kierunki, struktury, strategie i polityki, nie mówiąc o uwarunkowaniach i potencjałach (np. technicznych, finansowych, kadrowych itp.). Jest to zjawisko normalne. Początek rozwoju różnych krajów nie był przecież równoczesny, ich zasoby nie były jednakowe – historia, dziedzictwo kulturowe, postawy ludzi, obyczaje. Zróżnicowanie to zdaje się rosnąć, wbrew oczekiwaniom wynikającym z teorii postępu, teorii modernizacji, teorii imitacji czy uniwersalizmu, a także wbrew temu, czy mimo naśladownictwa, transferu wzorców, np. przez handel, wymianę, turystykę, media, migracje, integrację, globalizację. Powiększanie się cywilizacyjnej

różnorodności zdaje się jednak przeważać. Obecna wielotrajektoryjność i wielopoziomowość technoinformacyjnego rozwoju oraz zróżnicowanie jego efektów, skutków i ryzyka może być długofalowe. Różne poziomy i potencjały, różne strategie i polityki, nawet jeśli prowadzące w tym samym czy podobnym kierunku, będą dawać różne efekty[972].

TABELA 7.1. Przykładowy scenariusz zagrożeń w cyberprzestrzeni na szczeblu państwa

Typ działań destrukcyjnych	Skutek bezpośredni	Skutek dalszy	Przeciwdziałanie
Atak elektromagnetyczny, wyzwolenie impulsów elektromagnetycznych w rejonach węzłów sieci, uruchomienie urządzeń zakłócających pracę nadajników łączności bezprzewodowej	Zniszczenie urządzeń nadawczych telefonii bezprzewodowej elektronicznych i elektrycznych sieci teleinformatycznych, zakłócenie pracy lub paraliż tych sieci, zniszczenie stacji nadawczych telefonii komórkowej zakłócenia w pracy sieci, zakłócenie pracy stacji bezprzewodowej	Utrata informacji administracyjnych, zakłócenie pracy lub paraliż systemu administrowania miastem, wzrost poczucia zagrożenia i niezadowolenia społecznego	Wykrywanie i ocena zagrożeń, uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny, zorganizowanie systemu odtwarzania sprawności systemu po ataku
Atak ogniowy, zdetonowanie ładunków wybuchowych w obrębie węzłów sieci, przerwanie linii magistralnych sieci	Zniszczenie central telefonicznych i serwerowni – paraliż pracy sieci, zakłócenie pracy lub paraliż systemu administrowania miastem	Utrata informacji administracyjnych, zakłócenie pracy systemu administrowania państwem, wzrost poczucia zagrożenia i niezadowolenia społecznego	Wykrywanie i ocena zagrożeń, fizyczne uodpornienie sieci na atak ogniowy, zorganizowanie systemu odtwarzania sprawności systemu po ataku

Typ działań destrukcyjnych	Skutek bezpośredni	Skutek dalszy	Przeciwdziałanie
Działania psychologiczne, inżynieria społeczna – pozyskiwanie personelu urzędów do współuczestnictwa w atakach	Umożliwienie dostępu do sieci informatycznej systemów administrowania państwem, ujawnienie informacji niejawnej, sabotaż wewnętrzny ze strony pozyskanego personelu, defraudacje finansowe dokonywane przez pracowników administracji	Zewnętrzny atak informatyczny na sieć, zagrożenie bezpieczeństwa informacyjnego państwa, kradzież niejawnych informacji (np. danych osobowych czy finansowych), pogorszenie bezpieczeństwa finansowego, zakłócenia w administrowaniu państwem, wzrost poczucia zagrożenia i niezadowolenia społecznego	Wykrywanie i ocena zagrożeń, podnoszenie świadomości stanów osobowych, doskonalenie procedur kontroli dostępu do informacji
Dezinformacja, rozsyłanie fałszywych informacji pocztą elektroniczną oraz przez inne środki komunikowania społecznego	Kwestionowanie uczciwych zamiarów władz i kierownictw organizacji systemu administrowania państwem, podważanie wiarygodności oraz kwalifikacji wybranych grup personelu, rozpowszechnianie fałszywych informacji o zamiarach władz państwa, podawanie fałszywych informacji o pracy na rzecz interesów obcych państw i organizacji przez	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania państwa, próby zachwiania stabilnością finansową i płynnością finansową państwa, wzrost poczucia zagrożenia i niezadowolenia społecznego	Szybka reakcja władz na fałszywe informacje, sprawne docieranie do ludności i personelu firm z obiektywną informacją, zachowywanie prawdy w informowaniu, wykrywanie i piętnowanie dezinformatorów

Typ działań destrukcyjnych	Skutek bezpośredni	Skutek dalszy	Przeciwdziałanie
	przedstawicieli władz		

Źródło: P. Sienkiewicz, H. Świeboda, *Społeczna percepcja zagrożeń bezpieczeństwa obywatelskiego*, Warszawa 2005, s. 84–85.

Rozpatrując takie scenariusze dla przyjętego modelu systemu społecznego i hipotez dotyczących zmian społecznych oraz stosując metodę analizy prognostycznej GSO – technikę scenariuszy opierającą się na zestawie hipotetycznych zdarzeń, Piotr Sienkiewicz opracował trzy warianty rozwoju społeczeństwa informacyjnego[973]:

- wariant A – „system rozproszony" o strukturze sieciowej sprzyjającej „grze indywidualnych interesów", w którym podstawowymi zasobami są informacja i wiedza, zagrożeniem jest natomiast atomizacja zachowań społecznych wraz z „atrofią więzi" międzyludzkich;
- wariant B – „system zintegrowany" o strukturze liniowej i „grze grup interesów", której „wygraną" jest dostęp do wiedzy jako podstawowego zasobu, zagrożeniem może być swoisty „cyberautokratyzm" w przypadku uzyskania przez określoną grupę monopolu na wiedzę;
- wariant C – „system cybernetyczny" o strukturze nieliniowej sterowany „homeo- statycznie", sprzyjający dostępowi do wiedzy i mądrości pojmowanej jako zdolność do stosowania wiedzy w interesie całego społeczeństwa.

W nawiązaniu do wariantu A, rozszerzając analizę scenariusza w tym zakresie, należy zauważyć, że scenariusz ten przypomina wizję społeczeństwa orwellowskiego (pesymistycznego), gdzie społeczeństwo informacyjne będzie stanowić jedną z wielu możliwych konstrukcji będących zapewne idealizacją rzeczywistości społecznej, w której nie znikną tradycyjne problemy społeczne, np.:

- bezrobocie – rozwój IT będzie zapewne sprzyjał bezrobociu strukturalnemu;
- przestępczość – rozwiną się różne formy przestępczości informacyjnej;
- terroryzm, np. w postaci infoterroryzmu czy e-terroryzmu;

- rozwarstwienie społeczne jako wynik zróżnicowanego dostępu do szczególnie pożądanych zasobów;
- prymitywizacja kultury masowej, np. syndrom MTV, wirtualna rzeczywistość jako LSD XXI w.

Zapewne będzie kontynuowane dalsze zróżnicowanie, które przyniesie marginalizację czy nawet wykluczenie grup i jednostek (biednych, analfabetów, pozbawionych sprzętu i infrastruktury teleinformatycznej, niepełnosprawnych, chorych, w zaawansowanym wieku itp.). Mogą to być duże grupy (w krańcowych przypadkach niemal całe społeczeństwa, np. w tzw. najbiedniejszych czy „upadłych" krajach, choćby w Afryce). Nie zniknie też zapewne, mimo takich programów jak Europa 2020 czy Horyzont 2030, problem dywersyfikacji relacji online z tymi offline. *Digital divide* już istnieje, w najlepszym razie przesunie się na wyższy poziom. Wspomniana relacja może być trudna, tak jak relacja między zamożnymi a biednymi. Ewentualne zderzenia i konflikty wynikające ze zróżnicowania szans i możliwości rozwoju oraz dobrobytu mogą przyjmować sieciowe formy dewastujące globalną sieć i zwiększające nakłady na zabezpieczenia. Aspekty psychologiczne, społeczne, polityczne mogą sprawiać wiele kłopotów w kontekście głoszonego „optymizmu informacyjnego", możliwości współpracy sieciowej, zbiorowej inteligencji, wolnej kultury, bezpłatnego oprogramowania (*open source*, *free access* itp.), wolności internetowej[974].

Przestrzenią społecznych i ponadpaństwowych konfliktów będzie w rosnącym stopniu cyberprzestrzeń. Swoisty „wyścig zbrojeń" w tym obszarze może być bardzo kosztowny (w nakładach i skutkach). Trudną kwestią do prognozowania jest też relacja dwóch światów – rzeczywistego i wirtualnego. Będą się zmieniać ich proporcje różnie w poszczególnych krajach i społeczeństwach. W jednych świat realny będzie się coraz bardziej wirtualizował, świat wirtualny będzie się powiększał, będą one coraz bardziej powiązane i synergiczne w efektach (można to nazwać totalną wirtualizacją), w innych – świat wirtualny będzie raczej enklawą, niejako zewnętrzny, świat rzeczywisty zaś mało zwirtualizowany (z różnych przyczyn), czego efektem będzie suboptymalizacja rozwojowa czy niekompatybilności i frykcje rozwojowe, niewykorzystanie technicznych (*de facto* cywilizacyjnych)

okazji rozwojowych będzie więc generować lukę i w najgorszym przypadku ją petryfikować.

Kontrolowanie czy regulowanie prawne i polityczne wspomnianej relacji będzie zależeć od proporcji wielkości i siły obu światów. Założenie, że świat realny będzie dominował nad wirtualnym, odchodzi do lamusa. Nie znamy wszystkich możliwych narzędzi, jakimi w świecie wirtualnym będzie można wpływać na oba światy. Można przewidywać, że utrzyma się różnica – na wyższym poziomie technicznym – między światem liderów, modernizujących się, a resztą, tzw. współzależność rozwojowa jest czymś złożonym, niejednoznacznym, i to mimo procesów globalizowania się świata.

Scenariusz zintegrowany (wariant B) również można określić jako pośredni. Będzie dotyczył władzy i polityki, które w społeczeństwie informacyjnym nie znikają, ale informacyjnie mocno się modyfikują. Informacyjność przemian jest tu znacząca. Władza odchodzi od państwa narodowego ku globalnemu rynkowi i transnarodowym korporacjom, także organizacjom i instytucjom międzynarodowym (np. finansowym) oraz ku ustaleniom różnych „szczytów" (Ziemi, polityki i biznesu, rządów G8 czy G20). Wpływy mają też globalne organizacje obywatelskie, ruchy społeczne (np. Greenpeace, anty- i alterglobaliści). To wszystko jest możliwe dzięki technologiom informacyjnym. Wytwarza się więc nowe, sieciowe otoczenie czy raczej podłoże dla władzy i wpływów. Jest ono też podłożem społeczeństw informacyjnych. Co więcej, władza sięga i przechodzi do cyberprzestrzeni. Przestrzeń globalna i cyberprzestrzeń to nowe wyzwania dla rządzenia i polityki. „Obfitość informacyjna" pozwala na manipulacje, nieustanny marketing polityczny, public relations, postpolityczność[975]. Techniczne instrumenty są ważnym elementem substratu technicznego społeczeństwa informacyjnego. Oczekiwania upodabniania się kultur, ich integrowania się, zgodnego współistnienia, multikulturowości – pod naporem migracji z państw biednych, „innych" do bogatych – nie sprawdzają się. Etniczne grupy imigrantów nie wyrażają chęci do asymilowania się, nawet w Internecie chcą zachować swoją odrębność językową, obyczajową, kulturową, co wpływa na kształt społeczeństw informacyjnych z dużymi grupami imigrantów. Czy będą to społeczeństwa informacyjne etnicznie zróżnicowane w sieci? Globalny wymiar tego zjawiska to wielojęzyczność Internetu, którą część osób

uważa za jego koniec. W każdym razie sieć nie zapewnia pełnej uniwersalizacji oraz kulturowej dyfuzji i integracji, raczej umożliwia jednoczesność życia w wielu kulturach czy „przez kultury". Występuje zatem kolejny argument przemawiający za wizją mało wewnętrznie spójnej (informacyjnej) cywilizacji różnorodności.

Pojawia się również sztuczna inteligencja, która jest strategiczną technologią przynoszącą wiele korzyści obywatelom, przedsiębiorstwom, pod warunkiem że jest ukierunkowana na człowieka, etyczna, zrównoważona i przestrzega podstawowych praw oraz wartości. Może się również przyczynić do znalezienia rozwiązań części najpilniejszych wyzwań społecznych, w tym związanych z przeciwdziałaniem zmianie klimatu i degradacją środowiska, ze zrównoważonym rozwojem i zmianami demograficznymi oraz ochroną demokracji, a także – w razie potrzeby i w sposób proporcjonalny – przyczynić się do walki z przestępczością.

Aby Europa mogła w pełni wykorzystać możliwości oferowanych przez AI, musi rozwijać i wzmacniać niezbędne zdolności przemysłowe i technologiczne. Jak określono w europejskiej strategii, wymaga to również środków, które pozwolą UE stać się globalnym centrum danych. Europejskie podejście do sztucznej inteligencji powinno mieć na celu promowanie potencjału innowacyjnego Europy w tej dziedzinie, przy jednoczesnym wspieraniu rozwoju i wprowadzaniu etycznej i godnej zaufania sztucznej inteligencji w całej gospodarce unijnej. Sztuczna inteligencja powinna działać na rzecz ludzi i społeczeństwa.

Ostatni scenariusz (wariant C) dotyczy zróżnicowania generacyjnego i kulturowego. Nie ulega wątpliwości, że cechą społeczeństw ludzkich i kultur jest pluralizm systemów wartości. Pluralizm ten sprawia, że zarówno ludzkie bytowanie społeczne, jak i odpowiadająca mu refleksja teoretyczna są związane z niemal nieustannym dokonywaniem wyborów. Nie chodzi tu wyłącznie o wybory, które decydują o większych lub mniejszych różnicach w kierunku rozwoju technologicznego współczesnej cywilizacji, jakie pojawiają się w wypowiedzi Kuhna, a które znajdują się poza zasięgiem percepcji przeciętnych członków społeczeństw. Takie wybory mają bez wątpienia kluczowy charakter dla rozwoju cywilizacji. Właśnie ich istnienie zrodziło problem odpowiedzialności uczonego i tym podobne. Nauki społeczne mają

również do czynienia z różnorodnością systemów wartości, które są konstytutywnym elementem „codziennej" rzeczywistości społecznej[976].

To właśnie różnorodność systemów wartości wraz z wieloma innymi czynnikami decyduje o odmianach rzeczywistości, jakie obserwujemy w różnych okresach historycznych i w różnych szerokościach geograficznych. Uwypuklenie tego faktu jest niewątpliwie zasługą antropologii kulturowej. Wysiłki tej dyscypliny zmierzające do obalenia europocentryzmu w badaniu innych kultur przyniosły rezultaty, które bez wątpienia mają znaczenie również w odniesieniu do epistemologicznych problemów nauk społecznych. W ich rezultacie zagadnienie wartości – temat przewijający się w metodologii nauk społecznych od dawna, a szczególnie żywy co najmniej od czasów Rickerta[977] – zyskuje nową perspektywę. Kolejne generacje społeczeństw informacyjnych będą coraz bardziej „odstawać" od swoich poprzedników. Luki mogą być nie mniejsze niż między pierwszą generacją społeczeństwa informacyjnego a generacjami poprzedzającymi ją – społeczeństwa przemysłowego. Tak może się zdarzyć, jeśli technologie komunikacyjne będą rozwijać się w takim tempie jak dzisiaj czy skokowo (analogicznie do prawa Moore'a). Dzieci wychowujące się w środowisku cyfrowym są bardziej zaawansowane w nowych technologiach niż rodzice stosujący mniej lub bardziej efektywnie nowe technologie oraz niż wykluczeni dziadkowie i są znakiem czasów. Niekompatybilności psychologiczne, mentalne, edukacyjne, związane z umiejętnościami technicznymi, z wyobraźnią, sposobami kontaktowania się, z podzielanymi wartościami, stylem życia itp. mogą być znaczące i konfliktogenne w skali zarówno krajów, jak i międzynarodowej.

Technologia może więc być siłą dyferencjonującą, a nie uniwersalizującą kolejne pokolenia SI (ich mózgi i zachowania, ich *mindset* i *Weltanschauung*). Opisana wcześniej różnorodność kulturowa jest faktem. Tak jak różnią się regiony, państwa, społeczeństwa, jednostki ludzkie, tak różnią się ich zdolności kulturowe do tworzenia i stosowania techniki, w tym technologii informacyjnej.

W kontekście przyszłości społeczeństw postinformacyjnych i demokracji warto zwrócić uwagę na żądania, eksperymenty oraz praktyki demokratyzacji nauki i techniki oraz ich zastosowań. Wybory i decyzje w tych dziedzinach determinują tzw. substrat techniczny

społeczeństw informacyjnych, a więc demokratyzacja tych dziedzin przyczyniła się do rozwoju demokracji w społeczeństwach informacyjnych. W kontekście scenariusza dotyczącego polityki – w społeczeństwach i w skali globalnej – warto pamiętać o „systemowej ramie" rozwoju, czyli współczesnym kapitalizmie nazywanym technologicznym, informacyjnym, cyfrowym, kognitywnym czy nawet postkapitalizmem (Drucker). Wpływ tej ramy ma w dużej mierze charakter określający wiele parametrów ważnych dla rozwoju społeczeństwa postinformacyjnego, np. kwestii własności intelektualnej, relacji sfery prywatnej do publicznej, roli rynku i państwa, problemów nierówności. Jedno jest pewne – kapitalizm jako dominujący na świecie system będzie mieć istotny wpływ na kształt społeczeństw postinformacyjnych oraz informacyjnie nienadążających. Wpływ ten będzie zróżnicowany, podobnie jak jego efekty. Dla społeczeństw postinformacyjnych największe znaczenie będą miały takie wartości, jak informacja i satysfakcja. Transformacje kapitalizmu, które się wiążą z informacyjnością, cyfrowością, kognitywnością przybiorą zasięg międzyplanetarny, stawiając na pierwszym miejscu politykę energetyczną i ochronę środowiska. Tajemnica będzie miała wymiar organizacyjny, a nie handlowy.

W literaturze przedmiotu pojawiają się nowe pojęcia ilustrujące przemiany społeczeństw. Mówi się więc o e-społeczeństwie, e-stadzie, e-roju, inteligentnych tłumach, zespołach człowiek – maszyna[978]. Jeszcze bardziej prospektywne scenariusze opowiadają o nadchodzącej erze postinformacyjnej i następnie posthumanizmu, w którym era ludzka w tradycyjnym biologicznym rozumieniu się kończy. W dalszej perspektywie mówienie o społeczeństwach informacyjnych, przynajmniej w państwach najbardziej zaawansowanych technicznie i ekonomicznie, przestanie być sensowne, nawet gdy myśli się o społeczeństwach postinformacyjnych. Zastąpią je być może obiekty, systemy, procedury techniczne, zrobotyzowane, scyborgizowane, coraz mniej ludzkie. Wizje takie przestają być przedmiotem jedynie literatury fantastycznonaukowej, ale są wytworem twórców najnowszych technologii i ich najśmielszych wyobrażeń o przyszłości. Oni to tworzą rzeczowe elementy przyszłości i określają możliwości i kierunki rozwoju, które są przedmiotem badań AI.

Przytoczone scenariusze są w istocie bardzo ogólną wizją przyszłości. Myślenie o społeczeństwie informacyjnym wymaga postawy systemowej multi- i interdyscyplinarnej. Jest to bowiem problematyka wieloaspektowa zmuszająca do rozpatrywania aspektów humanistycznych, politycznych i społecznych, ekonomicznych i technicznych itp., obejmująca wszystkie sfery życia społecznego. Wszelkie odstępstwa czy pominięcia będą nadmiernym uproszczeniem, tak jak różne wizje (scenariusze) są tylko idealizacją rozwoju społeczeństwa informacyjnego. Racjonalizm analiz systemowych nakazuje analizę i ocenę szans i zagrożeń zarówno tych bliższych, jak i dalszych. Cóż z tego, że nakazuje, skoro możliwości naszego racjonalnego myślenia nie tylko o przyszłości, ale także o przeszłości systemów społecznych są tak dalece ograniczone. Jaki zatem będzie potencjał transformacyjny odnoszący się do świata, polityki, życia nowego pokolenia cyfrowego? Czy „dzieci komputera", „cyfrowi tubylcy" staną się „obywatelami sieci" (tzw. *netizens*) i sięgną po władzę, już tylko w sieci? Wreszcie czy będą zdolni do jakiejś autorefleksji i oceny swoich transformacji?[979]

ZAKOŃCZENIE

Technologia, zwłaszcza technologia informatyczna, rozwija się w szybkim tempie. Prawa międzynarodowe, regionalne i krajowe pozostają zawsze o krok za innowacjami technologicznymi. Postępu nie można zatrzymać, lecz należy spróbować skierować go na właściwe tory prawne.

Jacek Janowski[980] wyraził pogląd, że „abstrahując od zakresu regulacji określonych mianem prawa cyberprzestrzeni, można postulować zastosowanie go do unormowań stosunków nawiązywanych, utrzymywanych i modyfikowanych w cyberprzestrzeni". Podobne wnioski wyciągają eksperci, twierdząc, że tak jak niemożliwe jest odwrócenie zjawiska globalizacji ekonomicznej i informatycznej, tak nieunikniona okaże się perspektywa globalizacji prawa. Zagrożenia ekologiczne, przestępczość informatyczna czy światowy terroryzm zapewne przełożą się lub już się przekładają na oczekiwane powołania jakiejś postaci ponadpaństwowego porządku prawnego.

Do cech charakterystycznych cyberprzestrzeni należy: plastyczność, płynność, obliczalność, terytorialność, dokładność, hipertekstowość, interaktywność, wirtualność, kompatybilność, otwartość, nieograniczoność, ponadnarodowość, wszechstronność, złożoność, sieciowość, przenikalność, konwergencja, konsolidacja, automatyzacja i totalność. Cyberterroryści coraz częściej wchodzą w posiadanie najnowszych rozwiązań technologicznych, które umożliwiają im przeprowadzanie zdalnych ataków na wybrane cele drogami teleinformatycznymi. Ich specjaliści kształcą się na Zachodzie, tam zdobywają doświadczenie, by potem móc wykorzystywać je do wspierania działań terrorystycznych. Ataki cyberterrorystyczne mają wiele zalet dla potencjalnych napastników.

Dlatego podejmowane prace nad stworzeniem prawa cyberprzestrzeni muszą mieć charakter systemowy i odnosić się nie tylko do kwestii technicznych, ale także prawnych, ekonomicznych, społecznych i rozwojowych. Prawo powinno być tworzone z udziałem prawników, etyków, filozofów, twórców i specjalistów z branży IT. Została więc podjęta próba znalezienia odpowiedzi, w jakim stopniu powinno się tworzyć nowe rozwiązania prawne oparte na rozwoju technologii, a w jakim – na podstawie kryteriów ekonomiczno-społecznych, aby uzyskać ustanowienie reguł wzajemnej współpracy między Unią Europejską a państwami członkowskimi.

Współpraca między organami UE a państwami członkowskimi w zakresie zapewnienia bezpieczeństwa informatycznego nie jest prosta ze względu na znaczną liczbę systemów prawnych i różnorodnych inicjatyw podejmowanych w tym obszarze. Należy jednak wyraźnie zaznaczyć, że współpraca w tym zakresie nabrała tempa.

Na świecie przyjmuje się, że bardziej narażone na ataki z cyberprzestrzeni są systemy cywilne, ponieważ militarne posiadają lepsze zabezpieczenia. W polskich realiach ta reguła nie do końca się sprawdza. Nie zmienia to jednak faktu, że najbardziej zagrożonymi obszarami są systemy administracji państwowej, systemy bankowe, systemy wspomagające nadzór ruchu w sieciach transportowych, systemy sfery energetycznej, systemy kontroli lotów. Są to wybrane miejsca zagrożone atakami infoterrorystycznymi. Wszelkie podmioty będące elementami infrastruktury krytycznej państwa są narażone na większe niebezpieczeństwo.

Jest wiele technik cyberterrorystycznych (również cyberprzestępczych) i ich ewolucji. Ulegają one ciągłym przekształceniom wraz z rozwojem rynku zabezpieczeń. W zależności od postawionego celu napastnicy mogą wykradać informacje, zmieniać je, blokować serwery i strony internetowe, podmieniać treści na stronach internetowych. Efektów działalności cyberterrorystycznej w tym obszarze jest co najmniej tyle samo, ile technik.

W niniejszej publikacji dokonano analizy działań podjętych przez UE w polityce ochrony cyberprzestrzeni w celu zabezpieczenia wspólnej przestrzeni bezpieczeństwa informacyjnego UE w obliczu współczesnych zagrożeń. Przeprowadzono również analizę obecnej strategii cyberbezpieczeństwa, norm prawnych i polityki na tle standardów międzynarodowych w kierunku ustanowienia reguł wzajemnej współpracy między Unią Europejską a państwami członkowskimi.

Przedmiotem badawczym analizy była ochrona cyberbezpieczeństwa podejmowana w ramach polityki, strategii i prawa na poziomie zarówno Unii Europejskiej, jak i państwowym w związku ze zwalczaniem zagrożenia zjawiska, jakim jest cyberterroryzm. Analiza instytucjonalno-prawna ochrony cyberprzestrzeni w wybranych państwach UE pozwoliła ukazać, w jak różny sposób i z jaką efektywnością oraz szczegółowością można uregulować tę samą problematykę na szczeblu państwowym, będąc członkiem tej samej organizacji międzynarodowej, jaką jest UE, i będąc jednocześnie stroną tych samych konwencji międzynarodowych.

Konkludując, należy stwierdzić, że polityka ochrony cyberprzestrzeni jest reakcją powstałą na skutek braku odpowiednich działań i mechanizmów tym zakresie. To spowodowało, że UE zmierza do harmonizacji norm prawnych przyjętych w celu opracowania minimalnych standardów. Proces ten ewoluuje i nie można go uznawać za zakończony.

Należy też stwierdzić, że ewolucja ochrony cyberprzestrzeni, w tym polityki, strategii i prawa, jest reakcją na wzrost niestabilności i zagrożeń w tym obszarze i postępuje z różną prędkością w każdym państwie członkowskim. Wskazanie uwarunkowań zjawiska cyberterroryzmu w Unii Europejskiej pozwoliło stwierdzić, że przyczyną powstania tej polityki był również brak istnienia krajowych planów strategicznych w zakresie cyberbezpieczeństwa – jeszcze w 2012 r. nie więcej niż 12 państw miało stosowne strategie, w lipcu 2020 r. wszystkie państwa członkowskie je posiadają. W ciągle zmieniającym się środowisku cyberzagrożeń państwa członkowskie UE muszą mieć elastyczne i dynamiczne strategie

cyberbezpieczeństwa, aby sprostać nowym, globalnym zagrożeniom. Z kolei utworzenie określonych rodzajów mechanizmów i regulacji w tym obszarze daje podstawę do stwierdzenia, że mamy do czynienia zarówno z procesem instytucjonalizacji, jak i transformacji związanej z rewolucją przemysłową 4.0. i 5G.

Nie należy również zapominać, że Unia Europejska jako organizacja międzynarodowa implementuje w życie normy prawa międzynarodowego publicznego i działa, opierając się na ich podstawach. Podjęta próba wykazania, że to prawo unijne jest właściwym instrumentem służącym harmonizacji i uwspólnotowieniu regulacji prawa krajowego w cyberprzestrzeni została natomiast udowodniona, ponieważ to prawo unijne należy traktować jako *lex specialis* w stosunku do prawa międzynarodowego publicznego. Tym samym tworzone przez UE minimalne standardy w tym obszarze, oparte na normach prawa międzynarodowego publicznego (np. dyrektywa NIS opracowana na podstawie konwencji budapesztańskiej), są tego dobrym przykładem. Właśnie dlatego w dobie postępu zmian w środowisku międzynarodowym dotychczasowe postrzeganie bezpieczeństwa informacyjnego wymagało jego redefinicji, co zdecydowanie łatwiej było wprowadzić, opierając się na właściwych instrumentach harmonizacyjnych.

Należy również zauważyć, że zgodnie z art. 288 TL[981] transpozycja przepisów wprost z dyrektywy do prawa krajowego nie jest rozwiązaniem przyjętym przez ustawodawcę unijnego. Priorytetem jest spójność krajowego systemu prawa z prawem unijnym. Definicja bezpieczeństwa informacyjnego w dyrektywie NIS natomiast rozszerzyła podstawowe trzy atrybuty, tzn. poufność, integralność i dostępność, o czwarty, którym jest autentyczność, czyli właściwość polegająca na tym, że podmiot jest tym, za kogo się podaje[982]. Warto wspomnieć, że normy prawne są skuteczniej egzekwowane na poziomie prawa unijnego niż międzynarodowego.

Ponieważ zjawisko cyberterroryzmu ma charakter transgraniczny, polityka ochrony cyberprzestrzeni powinna nie tylko zwalczać zagrożenia cyberbezpieczeństwa, ale opierać się na współpracy

międzypaństwowej i koordynacji działań, które stanowią nieodzowny element skutecznej odpowiedzi na zagrożenie, jakim jest cyberterroryzm. Złożoność natury tego zjawiska powoduje jednak, że państwa muszą być elastyczne w reakcji na to zjawisko i zdolne do adaptacji zmieniających się warunków. Podjęto próbę wykazania, że pierwszoplanową rolę w skuteczności zwalczania zjawiska cyberterroryzmu odgrywa współpraca na poziomie zarówno państw członkowskich, jak i międzyinstytucjonalnym w poszczególnych państwach. Zostało to udowodnione, ponieważ w analizowanych strategiach państw największy nacisk położono właśnie na współpracę i tworzenie partnerstw publiczno-prywatnych (PPP) oraz reguł usprawniających współpracę międzypaństwową. W ten sposób zostaje potwierdzona teza, że im większy poziom wzmacniania współpracy między państwami i mechanizmów implementacji wewnątrzunijnych w obliczu zjawiska cyberprzestepczości, tym większe prawdopodobieństwo stabilności i bezpieczeństwa w UE i poszczególnych państwach.

Problemem pozostają nieścisłości prawne i rozbieżności interpretacyjne w zapisie regulacji prawnych na poziomie unijnym w zakresie podziału kompetencji dotyczących ochrony cyberprzestrzeni, które w rzeczywistości prowadzą do opóźnienia powstania wzajemnej współpracy między Unią a państwami członkowskimi. To z kolei może prowadzić do zjawiska „nadregulacji", ponieważ art. 73 TFUE wyraźnie dopuszcza możliwość stanowienia norm prawnych za zgodą państw na szczeblu unijnym. Jednocześnie zgodnie z art. 75 TFUE to zwalczanie terroryzmu i cyberterroryzmu znalazło się w obszarze kompetencji dzielonych UE i państw członkowskich, obszar cyberobrony jest natomiast podstawowym zadaniem i kompetencją państwa w polityce wewnętrznej państwa członkowskiego, co wynika z art. 4 wzw. 72 TFUE. Unii przyznano prawo do stanowienia strategii bezpieczeństwa w myśl art. 68 TFUE. W tej sytuacji prawnej państwa mogą, ale nie muszą uregulować kwestie związane z polityką cyberobrony. Na szczeblu unijnym może dojść do zjawiska nadregulacji i kolizji przepisów prawnych, co będzie negatywnie wpływało na proces usprawniania współpracy między państwami.

Odpowiadając na pierwsze i po części drugie z postawionych pytań badawczych, należy stwierdzić, że wprowadzenie mechanizmów współpracy dyrektywy 2016/1148 (NIS) na dwóch poziomach – technicznym i polityczno-strategicznym było właściwym i koniecznym posunięciem ze strony UE. Dyrektywa nałożyła także na państwa członkowskie obowiązek przyjęcia narodowej strategii bezpieczeństwa sieci i informacji, w której określone zostały m.in. narodowe cele i priorytety w dziedzinie cyberbezpieczeństwa, role i obowiązki organów administracji publicznej w procesie osiągania wyznaczonych celów, zasady współpracy sektorów publicznego i prywatnego oraz krajowa analiza ryzyka i zadania w zakresie edukacji na rzecz cyberbezpieczeństwa.

Przepisy dyrektywy umożliwiły utworzenie zarówno scentralizowanego systemu na poziomie państwowym, jak i podzielenie kompetencji między różne podmioty wymieniające informacje za pomocą wypracowanych mechanizmów współpracy. Dyrektywa zobowiązała także wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu krajowych zdolności w dziedzinie bezpieczeństwa teleinformatycznego. Dała organom publicznym konkretne narzędzie do przeciwdziałania i reakcji na incydenty w cyberprzestrzeni. Było to możliwe m.in. dzięki nałożonym obowiązkom raportowania, przygotowania krajowych strategii, skoordynowania przepływu informacji czy też zinstytucjonalizowania współpracy CSIRT.

Artykuł 83 TFUE umożliwia współpracę wymiarów sprawiedliwości w sprawach karnych oraz ustanowienie minimalnych zasad dotyczących definicji przestępstwa i sankcji w obszarach poważnych przestępstw o wymiarze transgranicznym, w tym przestępstw komputerowych. W związku z tym istnieje możliwość opracowania kolejnej ogólnej dyrektywy dotyczącej przemocy w cyberprzestrzeni, zawierającej definicje różnych rodzajów przemocy. Powinien nastąpić przegląd dyrektyw w sprawie praw ofiar przestępstw uwzględniający specyficzny charakter przemocy uwarunkowanej płcią i małoletniością oraz zawierać stosowne odniesienia do rozwiązań prawnych, które należałoby wprowadzić.

Najbliższa polityka cyberbezpieczeństwa Unii Europejskiej powinna zmierzać w kierunku zapewnienia bezpieczeństwa systemów informacyjnych, które są istotą bezpieczeństwa informacyjnego. Ze względu na znaczenie bezpieczeństwo informacyjne należy rozpatrywać w obszarach bezpieczeństwa organizacji i instytucji oraz obywatela. Wcześniej o kształcie obiegu informacji decydowała struktura społeczna. Obecnie nie tylko ona ma znaczenie, ponieważ w systemie informacyjnym wywierającym wpływ na społeczeństwo, oprócz struktur państwowych, występują także inne czynniki, m.in. środki masowego przekazu i cyberprzestrzeń.

Ponieważ uwarunkowania wewnętrzne UE są ściśle powiązane z odpowiednimi środkami wdrażanymi na poziomie operacyjnym, to taktyczna warstwa w WPBiO stanowi pierwszą linię obszarów cyberoperacji. Często warstwa ta nie ma zasobów ludzkich i zdolności lub działa w niesprzyjających warunkach również poza granicami UE. Dlatego ważne jest, aby móc zbudować dojrzałą cyberprzestrzeń, która jest elastyczna, skalowalna. Ważne jest również, aby była ona w stanie przekazywać wiarygodne informacje w niezawodny sposób do warstwy operacyjnej, jeśli chodzi o cyberzagrożenia w cyberoperacjach. Dlatego potrzebna jest współpraca w zakresie wymiany informacji i najlepszych praktyk między wojskowymi i cywilnymi zespołami WPBiO, prowadzenie kampanii uświadamiających skierowanych zarówno do pracowników WPBiO, jak i do obywateli UE mających na celu zwiększenie wiedzy na temat świadomości dotyczącej ochrony danych, prywatności i tożsamości, za pośrednictwem agencji takich jak ENISA.

Kończąc odpowiedź na drugie pytanie badawcze, należy stwierdzić, że na podstawie analizy aktów prawnych można wyciągnąć wniosek, że istniejące rozwiązania traktatowe są fragmentaryczne, a więc niewystarczające. Cyberprzestrzeń, jako dynamiczny obszar podlegający szybkim zmianom, jest krok przed normami prawa pozytywnego. Przestrzeń wirtualna nie może być jednak obszarem, w którym nie ma norm czy minimalnych standardów. Z tych względów część organizacji międzynarodowych proponuje rozwiązania modelowe, przyjmuje rezolucje i zalecenia,

które wskazują kierunki rozwoju prawa cyberprzestrzeni. Wydaje się, że właśnie *soft law* odgrywa ogromną rolę w kształtowaniu norm przestrzeni cyfrowej. Z jednej strony oddolne, nieformalne tworzenie norm odpowiada wolnościowemu charakterowi cyberprzestrzeni, z drugiej – w sposób stosunkowo szybki jest w stanie reagować na nowe wyzwania i dynamicznie zmieniającą się sytuację polityczną i technologiczną w globalnym świecie.

Na tej podstawie można wyprowadzić następujące wnioski badawcze i odpowiedzieć na postawione wcześniej pytania badawcze. Należy przede wszystkim poprawiać reakcję na incydenty cybernetyczne w ramach WPBiO oraz zwiększać ochronę infrastruktury krytycznej wykorzystywanej przez struktury WPBiO. Poprawy wymaga także system zarządzania kryzysowego w UE oraz cyberobrona. Niezbędne są również poprawa prawodawstwa dotyczącego cyberbezpieczeństwa i koordynacja egzekwowania prawa w zakresie cyberprzestępczości.

Kompleksowa, interdyscyplinarna analiza współczesnej polityki i strategii ochrony cyberprzestrzeni UE prowadzi do wniosku, że zjawisko to w ciągu ostatniej dekady niemal całkowicie zmieniło postać. Przeszło istotną dla społeczności międzynarodowej ewolucję. Z kolei analiza systemów ochrony prawa w cyberprzestrzeni na przykładzie wybranych państw UE pozwoliła wykazać, że będąc członkiem tej samej organizacji międzynarodowej, czyli UE, i jednocześnie stroną tych samych konwencji międzynarodowych, można w różny sposób i z różną efektywnością uregulować tę samą problematykę na szczeblach państwowych. Impulsem do przyśpieszenia rozwoju prawa i strategii w państwach UE był atak cybernetyczny w 2007 r. na Estonię, który można porównać do zamachu na WTC 11 września 2001 r. Analiza estońskiego porządku prawnego prowadzi do przekonania, że władze podejmują właściwe kroki w celu zapewniania bezpiecznego funkcjonowania społeczeństwa obywatelskiego, dając dobry przykład swoim sąsiadom zarówno przez wszechstronne regulacje prawne, jak i sam pomysł utworzenia cyberarmii.

Celem strategicznym polityki ochrony cyberbezpieczeństwa w analizowanych państwach członkowskich, Estonii, Francji,

Niemczech, Polsce i Wielkiej Brytanii, jest niwelowanie możliwości przeprowadzenia cyberataków przez aktorów państwowych i niepaństwowych oraz klasycznych zagrożeń o charakterze kryminalnym.

W Polsce przy dużej liczbie podmiotów bezpieczeństwa i porządku publicznego zauważalny jest brak pełnej koordynacji realizacji przypisanych im kompetencji, które często się nakładają. Szczególnie dokuczliwe jest powielanie kompetencji kierowniczych, które powinny zostać wyraźnie określone przez regulacje prawne. Mnogość podmiotów, a więc rozproszenie kompetencyjne, utrudnia kompleksowe rozpoznanie i identyfikację tego zagrożenia oraz efektywne dysponowanie siłami i środkami w celu przeciwdziałania tej przestępczości. Brak jednolitego sposobu rozliczania, ewidencjonowania i porównywania osiąganych wyników w kontekście nakładania się właściwości poszczególnych służb i podmiotów powoduje brak możliwości obiektywnej i porównywalnej oceny ich skuteczności[983].

Należałoby ujednolicić uprawnienia funkcjonariuszy różnych służb, procedury ich działania oraz pragmatyki służbowe. Rezultatem powinno być osiągnięcie sytuacji pozwalającej efektywnie dysponować posiadanym zasobem osobowym służb specjalnych, przy założeniu wymienności personelu między służbami oraz w procesie współdziałania. Na tym tle należy rozważyć propozycję uwolnienia służb specjalnych od obowiązków procesowych (powinny zostać przejęte przez CBŚ) i ograniczyć ich aktywność tylko do śledztw proaktywnych, tj. takich, które zmierzają do uprawdopodobnienia faktu popełnienia przestępstwa.

Moje zastrzeżenia budzi przede wszystkim dualizm regulacji w zakresie przyjętej właściwości odnośnie do konkretnych systemów i usług teleinformatycznych. Kolejną sprawą są bardzo szerokie uprawnienia CSIRT w zakresie możliwości żądania od operatorów telekomunikacyjnych udostępnienia informacji dotyczących działalności oraz przyjętych rozwiązań organizacyjno-technicznych. Wprowadzenie takich rozwiązań, w szczególności z pominięciem analizy ryzyka i bez uwzględnienia zasady adekwatności

stosowanych zabezpieczeń do zidentyfikowanych ryzyk, może w istotnym zakresie ograniczać swobodę działalności gospodarczej, a jednocześnie obniżać efektywność prowadzonych działań w obszarze cyberbezpieczeństwa.

Niemcy niewątpliwie należą do państw, które poważnie traktują zagrożenia cybernetyczne. W Republice Federalnej Niemiec opracowano nie tylko dokumenty o charakterze polityczno-programowym, jak *Strategia cyberbezpieczeństwa dla Niemiec* z 2011 r., ale także przyjęto ustawę, która porządkuje kompetencje organów i systematyzuje proces zapewniania bezpieczeństwa IT.

W niewielu państwach funkcjonuje podobne kompleksowe rozwiązanie prawne w omawianej dziedzinie. Warto dodać, że RFN stara się, aby przyjmowane rozwiązania były zgodne z wytycznymi międzynarodowymi. Pozytywną cechą systemu stworzonego przez Niemcy jest wysoki stopień włączenia w tworzenie bezpieczeństwa cybernetycznego prywatnych operatorów infrastruktury krytycznej. Są oni nie tylko wykonawcą licznych obowiązków ustawowych, ale także partnerem, m.in. w ramach Narodowej Rady Cyberbezpieczeństwa. Na mocy ustawy z 2015 r. biznes może również wprowadzać rozwiązania w typie samoregulacji.

Odnosząc się do istniejącej siatki organów i instytucji zajmujących się bezpieczeństwem cybernetycznym, należy stwierdzić, że słowem-kluczem jest koordynacja. Istnieje platforma współpracy między organami cywilnymi i wojskowymi. Specyficzną cechą niemieckich rozwiązań jest powierzenie BSI kontroli nad sposobem wdrożenia szczegółowych procedur ochronnych w tych działach infrastruktury krytycznej, które decydują o sposobie funkcjonowania społeczeństwa. Jest to efektywne rozwiązanie zapobiegające dublowaniu kompetencji oraz pułapki braku adresata ważnej informacji.

Niemieckie rozwiązania powodują, że system bezpieczeństwa cybernetycznego koncentruje się na ochronie infrastruktury krytycznej, elementach technologii informatycznych i komunikacyjnych oddziałujących na sposób funkcjonowania społeczeństwa oraz Internet. Za najpoważniejsze zagrożenie uznano cyberataki, cyberszpiegostwo oraz sabotaż. Na wypadek wojny w

cyberprzestrzeni strategia pokazuje, że omawiany aspekt nie jest pomijany, choć wciąż wydaje się, że zdolności te traktowane są defensywnie lub jako instrument wspierający działania regularnego wojska, np. podczas zagranicznych misji i operacji.

Przykład Wielkiej Brytanii potwierdza z kolei, że jej polityka i instrumenty prawne oraz strategia z 2016 r. w zakresie ochrony cyberprzestrzeni stawiają na prewencję będącą najlepszym środkiem ochronnym. To czyni Brytyjczyków ważnym graczem (supermocarstwem) w cyberprzestrzeni Europy i świata. Żadnemu innemu państwu, mimo wielu założeń, nie udało się dotychczas wypracować pozycji supermocarstwa Europy, a Wielka Brytania od 2018 r. plasuje się na drugiej pozycji. Jest to dowód, że instrumenty zastosowane w realizacji polityki ochrony cyberprzestrzeni przez Wielką Brytanię okazały się najwłaściwsze.

Należy jednak pamiętać, że opracowana strategia cyberprzestrzeni była pierwszą w dziejach Wielkiej Brytanii i jedną z pierwszych na świecie. Miała wyznaczać główne trendy w dziedzinie bezpieczeństwa cybernetycznego, a nie proponować konkretne rozwiązania. Powołała również Biuro Cyberbezpieczeństwa i Centrum Operacji Cybernetycznych.

Zaletą Wielkiej Brytanii jest bardzo precyzyjny podział kompetencji między poszczególne instytucje oraz tworzenie stosownych narzędzi prawnych typu *bulk* w celu neutralizacji zagrożenia przez jego monitorowanie i wykorzystywanie urządzeń teleinformatycznych. Wielka Brytania jest państwem, które posiada najmniej regulacji prawnych w zakresie cyberterroryzmu, jednak są one bardzo precyzyjne i w większości dotyczą zwalczania przyczyny, która ma źródło również poza granicami państwa.

Z kolei Republika Francuska jest jedynym państwem Unii Europejskiej, w której celem polityki bezpieczeństwa cybernetycznego jest zarówno rozwój zdolności o charakterze ofensywnym, pozwalających na wsparcie operacji wojskowych, jak i podkreślenie znaczenia gospodarczego wymiaru cyberbezpieczeństwa oraz potencjalnych skutków, jakie mógłby wywołać ewentualny atak informatyczny na systemy wykorzystywane przez najważniejsze przedsiębiorstwa. Takie ujęcie

powoduje, że podsystem militarny ochrony cybernetycznej funkcjonuje samodzielnie, a w jego ramach prowadzone są działania o charakterze defensywnym, w zasadzie ukierunkowanym na ochronę wojskowej infrastruktury informatycznej, oraz ofensywnym, ale ich zasadniczym celem jest zapewnienie tzw. suwerenności informacyjnej tego kraju. Warto zauważyć, że Francja stara się konkurować w tym obszarze z Wielką Brytanią.

Problemem Francji jest mnogość ustaw i przepisów stanowiących podstawę prawną zwalczania zjawiska cyberterroryzmu i, podobnie jak w Polsce, mnogość podmiotów, a więc rozproszenie kompetencyjne. Utrudnia to kompleksowe rozpoznanie i identyfikację tego zagrożenia oraz efektywne dysponowanie siłami i środkami w celu przeciwdziałania tej przestępczości. We Francji są dwa głównodowodzące podmioty w tym obszarze polityki, czyli prezydent i premier, a każdy odpowiada za inny organ, co w przypadku systemu semiprezydenckiego może wiązać się ze zjawiskiem *cohabitation (*koabitacji) i w przypadku zaistnienia nie będzie korzystnie wpływać na politykę ochrony cyberprzestrzeni Francji.

Przedstawione scenariusze rozwoju społeczeństwa informacyjnego pozwalają skłaniać się w stronę scenariusza pośredniego, ponieważ jesteśmy społeczeństwem informacyjnym. Jego globalny wymiar to wielojęzyczność sieci i sztuczna inteligencja, która jest strategiczną technologią przynoszącą wiele korzyści obywatelom, przedsiębiorstwom, ale pod warunkiem że jest ukierunkowana na człowieka, etyczna, zrównoważona i przestrzega podstawowych praw i wartości. Może się również przyczynić do znalezienia rozwiązań niektórych najpilniejszych wyzwań społecznych, w tym związanych z przeciwdziałaniem zmianie klimatu i degradacją środowiska, ze zrównoważonym rozwojem i zmianami demograficznymi oraz ochroną demokracji. Może się też przyczynić do walki z cyberprzestępczością.

BIBLIOGRAFIA

Dokumenty

Biała Księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania (COM(2020) 65 final, 19.02.2020).

Communication from Commission to the Council and the European Parliament: Development of Schengen Information System II (COM(2001) 720, 18.12.2001).

Communication from the Commission to the Council and the European Parliament Implementing The Hague Programme: the way forward (COM(2006) 331 final, 28.06.2006).

Communication from the Commission to the European Parliament, the Council and the Committee of the regions towards a general Policy on the fight against cyber crime Com/2007/0267 Final Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention) (Dz.Urz. WE C 316 z 27.11.1995).

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, On Fighting Spam, Spyware and Malicious Software (COM(2006) 688 final, 15.11.2006).

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Reference, CETS No. 108 (1981); http://www.coe.int/pl/web/conventions/full-list/-/conventions/treaty/108 (dostęp: 06.07.2020).

Council Resolution of 21 December 1998 on the prevention of organised crime with reference to the establishment of a comprehensive strategy for combating I (Dz.Urz. WE C 408 z 13.12.1998).

Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (Dz.Urz. EU L 190 z 18.07.2002).
Cybersecurity in the EU Common Security and Defence Policy (CSDP) Challenges and risks for the EU. Study, dok. RS/STOA/SER/16/214N, Brussel 2017.
Decyzja Komitetu Stałych Przedstawicieli z dnia 13 czerwca 2001 r. ustanawiająca grupę roboczą wysokiego szczebla (Dz.Urz. WE C 183 z 29.06.2001).
Decyzja Rady 2002/187/WSiSW z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością (Dz.Urz. EU L 63 z 06.03.2002).
Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.Urz. EU L 205 z 07.08.2007).
Decyzja Rady 2008/633/WSiSW85 uzupełnia rozporządzenie w sprawie VIS w zakresie dotyczącym dostępu wyznaczonych organów państw członkowskich i Europolu (VIS) (Dz.Urz. EU L 218 z 13.08.2008).
Decyzja Rady nr 2011/318/WPZiB z 31 marca 2011 r. w sprawie podpisania i zawarcia umowy ramowej między Stanami Zjednoczonymi Ameryki a Unią Europejską w sprawie udziału Stanów Zjednoczonych Ameryki w operacjach zarządzania kryzysowego prowadzonych przez Unię Europejską (Dz.Urz. EU L 143 z 31.05.2011).
Decyzja Rady 2002/187/WSISW ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością (Dz.Urz. EU L 63 z 5.03.2002).
Decyzja Rady z dnia 20 września 2005 r. w sprawie wymiany informacji i współpracy
Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz.Urz. EU L 69 z 16.03.2005).
Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach

współpracy policyjnej i sądowej w sprawach karnych (Dz.Urz. EU L 350 z 30.12.2008).
Decyzja Rady 2006/1007/WSiSW z dnia 21 grudnia 2006 r. zmieniająca decyzję 2001/886/WSiSW w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji (SIS II).
Decyzja dotycząca przestępstw terrorystycznych (Dz.Urz. EU L 253 z 29.09.2005).
Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.Urz. WE L 178 z 17.07.2000).
Dyrektywa 2002/22/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników (dyrektywa o usłudze powszechnej) (Dz.Urz. EU L 108 z 24.04.2002).
Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. EU L 201 z 31.07.2002).
Dyrektywa 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu (Dz.Urz. EU L 309 z 26.10.2005).
Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz.Urz. WE L 281 z 23.11.1995).
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, źródło: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32016L1148&from=EN (dostęp: 19.04.2018).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona) (Dz.Urz. EU L 321, 17.12.2018).
Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.Urz. EU L 335 z 17.12.2011).
Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. EU L 218 z 14.08.2013).
Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych (Dz.Urz. EU L 130 z 1.05.2014).
Dyrektywa Rady 2008/114/WE z grudnia 2008 r. w sprawie europejskiej infrastruktury krytycznej (Dz.Urz. EU L 345 z 23.12.2008).
Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz.Urz. EU L 345 z 23.12.2008).
Dyrektywa Parlamentu Europejskiego i Rady UE nr 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. EU L 194 z 19.07.2016).
eEurope 2002 – An Information society for all – Draft Action Plan prepared by the European Commission for the European Council in Feira, 19–20 June 2000 (COM(2000) 0330 final).
eEurope 2005: An information society for all (COM(2002) 263 final, 28.05.2002).
Europe and the Global Information Society. Recommendations of the Bangemann Group to the European Council, Brussels, 26 maja 1994.

European Union, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML (dostęp: 16.07.2020).

European Union, *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services*; *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws*; http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009L0136 (dostęp: 16.07.2020).

European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Brüssel 1995; http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046 (dostęp: 20.07.2020).

Europejska Strategia Bezpieczeństwa. Bezpieczna Europa w lepszym świecie, Bruksela 2009.

Europejski nakaz aresztowania O.J.C. 140 E, 13.06.2002 r.

Europol, Cybercrime: improving international cooperation. GCCS2015 Parallel session 4. Discussion paper. www.enisa.europa.eu/activities/cert/events/files/ENISA_Europol_threat_assessment_2007_Dileone.pdf (dostęp: 08.07.2019).

i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia (COM(2005) 229, 01.06.2005).

II *Preparatory Acts pursuant to Title VI of the Treaty on European Union.*

2001/C 328/12 O.J.L. 328, 13.12.2001 r.

International review of criminal Policy. 1994, No. 43–44 (UN. Centre for Social Development and Humanitarian Affairs.
Klauzule UE o wzajemnej obronie i solidarności: wymiar polityczny i operacyjny, „Dziennik Urzędowy Unii Europejskiej", źródło: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52012IP0456 (dostęp: 02.07.2019).
Komisja Europejska, *Dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych; Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych* (COM(2012) 11 final).
Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Europejska agenda cyfrowa (COM(2010) 245 final, 16.05.2010).
Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Zamknięcie obiegu – plan działania UE dotyczący gospodarki o obiegu zamkniętym*, źródło: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52015DC0614 (dostęp: 12.07.2019).
Komunikat Komisji, *State of the Union 2017: The Commission scales up its response to cyberattacks,* 2017, źródło: europa.eu/rapid/press-release_MEMO-17-3194_en.pdf (dostęp: 19.04.2018).
Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Zamknięcie obiegu – plan działania UE dotyczący gospodarki o obiegu zamkniętym, źródło: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52015DC0614, (dostęp: 12.07.2020).
Konkluzje Rady w sprawie Komisji i Wysokiego Przedstawiciela UE. Wspólna komunikacja Unii Europejskiej do spraw zagranicznych i

polityki bezpieczeństwa w sprawie Strategii Cyberbezpieczeństwa Unii Europejskiej: Otwarta i bezpieczna cyberprzestrzeń, Dokument nr 11357/13, Bruksela 22.07.2013 r.
Konwencja Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 15 listopada 2000 r. (Dz.U. z 2005 r. Nr 18, poz. 158).
Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz.U. z 2003 r. Nr 3, poz. 25).
Green Paper. Living and Working in the Information Society: People First (COM(96) 389 final, 24.06.1996).
NATO StratCom COE, *2007 cyber attacks on Estonia.*
Organisation for Economic Cooperation and Development (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris 1980.
Plan działań w zakresie zwalczania terroryzmu przyjęty przez nadzwyczajne posiedzenie Rady Europejskiej w Brukseli 21 września 2001 r., decyzja ramowa Rady Europejskiej 2002/475/WSiSW z 13 czerwca 2002 r. w sprawie zwalczania terroryzmu, decyzja ramowa w sprawie europejskiego nakazu aresztowania i procedury wydawania osób miedzy państwami członkowskimi, w: *Terroryzm: europejska riposta,* Komisja Europejska, Dyrekcja Generalna ds. Sprawiedliwości, Wolności i Bezpieczeństwa, Bruksela, sierpień 2004 r., http://ec.europa.eu/justice_home/key_issues/terrorism/terrorism_0904_pl.pdf. (dostęp: 8.07.2020).
Policy paper. Foreign policy, defence and development – a future partnership, paperhttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643924/Foreign_policy__defence_and_development_paper.pdf (dostęp: 30.07.2020).
Plan działania Rady i Komisji służący realizacji programu haskiego mającego na celu wzmacnianie wolności, bezpieczeństwa

i sprawiedliwości w Unii Europejskiej O.J.C. 198 z 12.08.2005 r.
Program sztokholmski. Otwarta i bezpieczna Europa dla dobra i ochrony obywateli, Dz.Urz. EU UE 2010 C 115.
Proposal for a Council regulation amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (COM[2002]406 – C5-0433/2002 2002/0173[CNS]).
Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data COM(2012) 10 final, dokument z 25.01.2012.
Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych sporządzony w Strasburgu 8.11.2001 r. (Dz.U. z 2006 r. Nr 3, poz. 15).
Protokół Rady 2003/659/ WSiSW z dnia 18 czerwca 2003 r. (Dz.Urz. EU L 245 z 29.09.2003).
Regulation of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (EU) no 526/2013 (CYBERSECURITY ACT), Dok. PE-CONS 86/1/18 REV 1(2017/0225 (COD) LEX 1899).
Rezolucja przyjęta przez Sekretarza Generalnego 27 grudnia 2013 r. (A/RES/53/70).
Rezolucja Rady Gospodarczej i Społecznej ONZ przyjęta w lipcu 2011 r. (E/2011/30).
Rezolucja ustawodawcza w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową Rady 2005/222/WSISW (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)).

Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ENISA, „Agencji ds. Bezpieczeństwa cybernetycznego w UE" i uchylającego rozporządzenie (UE) 526/2013 oraz w sprawie certyfikacji cyberbezpieczeństwa technologii informacyjnych i komunikacyjnych („Ustawa o cyberbezpieczeństwie"), źródło: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0477:FIN (dostęp: 19.04.2018).
Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (Dz.Urz. EU L 77 z 13.03.2004).
Rozporządzenie Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznające niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz.Urz. WE C 187 z 03.07.2001).
Rozporządzenie Komisji (WE) nr 425/2005 z dnia 15 marca 2005 r. zmieniające rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 998/2003 w odniesieniu do wykazu państw i terytoriów (Dz.Urz. EU L 69 z 16.03.2005).
Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004 (Dz.Urz. EU L. 165 z 18.06.2013).
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz. EU L 151 z 7.06.2019).
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. EU L 119 z 4.05.2016).
Rozporządzenie (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia,

funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.Urz. EU L 381 z 28.12.2006).
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. EU L 119 z 04.05.2016).
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz. EU L 151 z 7.06.2019).
Rozporządzenie Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz.Urz. EU L 129 z 17.05.2019).
Rozporządzenie Rady (WE) nr 1988/2006 z dnia 21 grudnia 2006 r. zmieniające wcześniejsze rozporządzenie nr 2424/2001 w sprawie rozwoju SIS II (Dz.Urz. EU L z 2.02.2007).
Rozporządzenie Rady (WE) nr 2580/2001 z dnia 27 grudnia 2001 r. w sprawie szczególnych środków restrykcyjnych skierowanych przeciwko niektórym osobom i podmiotom mającym na celu zwalczanie terroryzmu (Dz.Urz. EU L 344 z 28.12.2001).
Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady z postępu prac nad systemem informatycznym Schengen drugiej generacji (SIS II) styczeń 2011 r.czerwiec 2011 r. (COM(2011) 907 final).
Statut Rady Europy, przyjęty w Londynie dnia 5 maja 1949 r. (Dz.U. z 1994 r. nr 118, poz. 565).
Strategy Paper and Report of the European Commission on the progress towards accession by each of the candidate countries (COM[2002] 281 final)
The Hague Programme: strengthening freedom, security and justice in the European Union The Hague (Dz.Urz. EU C. 53 z 03.03.2005).
Traktat o Unii Europejskiej (Dz.Urz. UE C 191 z 29.7.1992)

Traktat z Amsterdamu z 2 października 1997 r. (Dz.Urz. WE C 340 z 10.11.1997).
Traktatu z Nicei z 26 lutego 2001 r. (Dz.Urz. UE C 235 z 24.12.2002).
Uzasadnienie do Rady decyzją Rady powierzającą agencji ustanowionej na mocy rozporządzenia XX zadania dotyczące zarządzania operacyjnego systemami SIS II i VIS w zastosowaniu tytułu VI Traktatu UE (COM/2009/0294 końcowy – CNS 2009/0090).
Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie „Agencji UE ds. Cyberbezpieczeństwa" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt ws. Cyberbezpieczeństwa" (COM(2017) 477).
Wspólne działanie z 15 października 1996 r. przyjęte przez Radę na podstawie art. K.3 Traktatu o Unii Europejskiej, dotyczące utworzenia i utrzymywania spisu na temat szczególnych uprawnień antyterrorystycznych, umiejętności i wiedzy specjalistycznej ułatwiających współpracę antyterrorystyczną między państwami członkowskimi Unii Europejskiej (Dz.Urz. WE L 273 z 25.10.1996).
Wspólne działanie z 21 grudnia 1998 r. przyjęte przez Radę na podstawie art. K.3 Traktatu o Unii Europejskiej, w sprawie uznawania za przestępstwa karne uczestnictwa w organizacji przestępczej w państwach członkowskich Unii Europejskiej (Dz.Urz. WE L 351 z 29.12.1998).
Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (JOIN(2013) 1 final, 7.02.2013).
Wyzwania w zakresie bezpieczeństwa, z jakimi Europa musi się zmierzyć w przyszłości, Bruksela, 20 czerwca 2014 r. (IP/10/1535 i MEMO/10/598).
93 Europe and the Global Information Society. Recommendations of the Bangemann Group to the European Council, Brussels, 26 maja

1994 r.

Orzecznictwo

Wyrok ETS z 13.09.2005 r. w sprawie C-176/03 Komisja v. Rada.
Wyrok ETS z 23.10.2007 r. w sprawie C-440/05 Komisja p. Rada.
Wyrok ETS z 16.07.2020 r. w sprawie C-496/19 Antonio Capaldo.
Wyrok ETS z 03.05.2007 r. w sprawie C-303/05, Advocaten voor de Wereld p. Leden.
Wyrok ETS z 25.10.2011 r. w sprawie *C-509/09* eDate Advertising v. Marines.
Wyrok ETS z 05.04.2016 r. w sprawie C-404/15 Aranyosi i Căldăraru.
Wyrok TS z 21.01.2020 r. w sprawie C-274/14 Banco de Santander.
Wyrok TS z 26.03.2020 r. w sprawie C-558/18 miasto Łowicz i prokurator generalny.
Wyrok SPI z 01.10.2005 r. w sprawie T-229/02 PKK v. Rada.
Wyrok ETPC z 30.08.1990 r. w sprawie Fox, Campbell i Chartley v. Wielka Brytania.
Wyrok ETPC z 15.11.1966 r. w sprawie Clauhal v. Wielka Brytania.
Wyrok ETPC z 18.12.1966 r. w sprawie Aksoy v. Turcja.
Wyrok ETPC z 18.01.1978 r. w sprawie Irlandia v. Wielka Brytania.
Wyrok ETPC z 07.07.1989 r. w sprawie Soering v. Wielka Brytania.
Wyrok ETPC z 27.08.1992 r. w sprawie Tomasi v. Francja.
Wyrok ETPC z 28.10.1994 r. w sprawie Murray v. Wielka Brytania.
Wyrok ETPC z 27.09.1995 r. w sprawie McCann i inni v. Wielka Brytania.
Wyrok ETPC z 02.09.1998 r. w sprawie Yasa v. Turcja.
Wyrok ETPC z 28.07.1998 r. w sprawie Ergi v. Turcja.
Wyrok ETPC z 29.03.2010 r. w sprawie nr 3394/03 (Medvedyev v. Francja).
Orzeczenie Sądu Okręgowego w Paryżu z 20.10.2000 r. w sprawie Anit-Semitism LICRA v. Yachoo! Inc., sygn. akt No RG 00/05308. 200.
Wyrok Yahoo! v. La Ligue Contre le Racisme et l'Antisémitisme, sygn. akt 2006 WL 60670 (9th Cir. 2006) C-00-21275 JF.
Wyrok Cour d'appel w Paryżu z 27.09.2006 r., nr 04-20185.

Wyrok Sądu Kasacyjnego we Francji z 09.12.2003 r., Cour de cassation nr 01-03225.
Wyrok Sądu Apelacyjnego House of Lords z 10.04.1997 r. w sprawie R. v. Governor of Brixton Prison and another, ex parte Levin, sygn. akt. 4 All ER 350, All ER 289.
Uchwała SN z 22.01.2003 r., I KZP 43/02, OSNKW 2003, nr 1 poz.5.
Wyrok SN z 26.10.1938 r., sygn. akt 1 K 2813/37, Zb. Orz. SN 1939, nr 6, poz. 135.
Wyrok SN z 3.6.1996 r., sygn. akt II KKN 24/96.
Wyrok SN z 5.01.2001 r., V KKN 504/00, OSNKW 2001/7–8.
Wyrok NSA z 18.11.2009 r., I OSK 667/09.
Wyrok SA Kraków z 19.12.2000 r., I ACa 794/00, TPP 2002, nr 3.
Postanowienie NSA z 23.04.2020 r. w sprawie II GZ 97/20.
Wyrok WSA z 11.12.2019 r. w sprawie VI SA/Wa 1436/19.

Najważniejsze dokumenty Estonii

Estońska ustawa o łączności elektronicznej 8 grudnia 2004 r. (RT I 2004, 87, 593).
Estońska ustawa o ochronie danych osobowych z dnia 6 grudnia 2007 r. (RT I 2007, 68, 421).
Estońska ustawa o cyberprzestrzeni (RT I, 22.05.2018).
Estoński National Defence Act (RT I, 01.04.2016).
Estońska Strategia Cyberbezpieczeństwa na lata 2014–2017.
Estońska Strategia Cyberbezpieczeństwa na lata 2008–2013.
Estońska Doktryna Obrony Państwa.
Strategia Cyberbezpieczeństwa Estonii na lata 2019–2022.

Najważniejsze dokumenty Francji

Code de la sécurité intérieure (JO du 31/07/2020 version consolidée).
Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portent diverses dispositions concernant la défense et la sécurité nationale.
Loi n ° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
Loi n° 2012-410 du 27 mars 2012 relative à Code penal.

Le décret núm. 2002–890 du 15 mai 2002 relatif au Conseil de sécurité intérieure.
Le décret núm. 89–258 du 20 avril 1989, le CIR est chargé d'assurer l'orientation et la coordination des activités des services qui concourent au renseignement.

Najważniejsze dokumenty Polski

Konstytucja RP (Dz.U. z 1997 r. nr 78, poz. 483 z późn. zm).
Dyrektywa Parlamentu Europejskiego i Rady 2016/1148/UE z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. EU UE L 194 z 19.07.2016).
Ustawa z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 762.).
Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz.U. z 2019 r. poz. 945 z późn zm.)
Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2019 r. poz. 1398 z późn. zm.).
Ustawa o ABW z dnia 24 maja 2002 r. (Dz.U. z 2002 r. Nr 93, poz. 829).
Ustawa o Policji z dnia 6 kwietnia 1990 r. (Dz.U. 1990 r. Nr 30, poz. 179 ze zm.).
Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. z 2016 r. poz. 904 oraz z 2018 r. poz. 452, 650 i 730).
Ustawa o Agencji Wywiadu (Dz.U. z 2017 r. poz. 1920 i 2405 oraz z 2018 r. poz. 138, 650, 723 i 730).
Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 16 listopada 2000 r. (Dz.U. z 2003 r. Nr 153, poz. 1505 z późn. zm.).
Ustawa z 12 października 1990 r. o Straży Granicznej (Dz.U. z 2005 r. nr 234, poz. 1997 ze zm.).
Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2017 r. poz. 209 i 1566).
Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138 i 650).

Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. z 2017 r. poz. 1876, 2361 i 2491 oraz z 2018 r. poz. 62, 106, 138, 650, 685 i 723).
Kodeks karny (Dz.U. 1997 r. nr 90, poz. 557 z późn. zm.).
Konwencja budapeszteńska z 23 listopada 2001 r. (Dz.U. 2014 r. poz. 1514).
Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247).
Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2013 (https://www.bialystok.ap.gov.pl/arch/teksty/biala_ksiega.pdf).
Doktryna cyberbezpieczeństwa Rzeczypospolitej z 22 stycznia 2015 r.
Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022.
Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej z 25 czerwca 2013 r.
Strategia bezpieczeństwa z 9 kwietnia 2013 r.
Strategia Bezpieczeństwa Narodowego (SBN) z 2014 r.
Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.
Strategia Bezpieczeństwa Narodowego, Warszawa 2020. (https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf)

Najważniejsze dokumenty RFN

Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen, Bundesministerium des Innern, Berlin 2007, s. 10.
Cyber Security Strategy for Germany, Bundesministerium des Innern, Berlin 2011, s. 11 i n.
Nationale Strategie zum Schutz Kritischer Infrastrukturen, Bundesministerium des Innern, Berlin 2009, s. 5–6.

Cyber-Sicherheitsstrategie für Deutschland 2016, Bundesministerium des Innern, Berlin 2016, s. 4–9.
Konwencja Rady Europy o cyberprzestępczości sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r. poz. 728).
Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015, (BGBI. I S. 1324).
Germany passes strict cyber-security law to protect „critical infrastructure", https://www.rt.com/news/273058-german-cyber-security-law/ (dostęp: 07.07.2017).
Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg, 2015, https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/#Strategische-Leitlinie-Cyber-Verteidigung (dostęp: 07.07.2017).
Strafgesetzbuch (StGB) vom 15.05.1871 (BGBI, I s. 3083).
Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG) vom 20 Dezember 1990 (BGBI. s. 2576).
Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (Zivilschutz- und Katastrophenhilfegesetz – ZSKG) vom 25.03.1997 (BGBl. I S. 726).
Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt z 25.12.2008 r. BGBI. I, s. 3083).
Gesetz über den Bundesnachrichtendienst (BND – Gesetz – BNDG) vom 20 Dezember 1990 (BGBI. S. 2576).
Überblick:Cyber-Abwehr der Bundeswehr, http://www.bmvg.de/ *(*dostęp: 07.07.2017).
Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009 (BGBl. I S. 2821).
Urheberrechtsgesetz (UrhG) vom 09.09.1965 (BGBI, I s. 3037).
Strafgesetzbuch (StGB) vom 15.05.1871 (BGBI, I s. 3083).

Najważniejsze dokumenty Wielkiej Brytanii

Computer Misuse Act z 1990 r. (UK Public General Acts 1990 c. 18).
Investigatory Powers Act 2016.
Regulation of Investigatory Powers Act 2000.
Strategia Cyberbezpieczeństwa Wielkiej Brytanii z dnia 25.11.2011 r. lata 2011–2016.
Strategia bezpieczeństwa cybernetycznego Wielkiej Brytanii z 30.11.2016 r. na lata 2016–2021.
The National Security strategy of the United Kingdom, 2009.

Statystyka

APWG Phishing Activity Trends Report 4th Quarter of 2017, http://www.apwg.org (dostęp: 27.05.2018).
Cyber Security Report 2020, https://research.checkpoint.com (dostęp: 30.06.2020).
Cyber_Security_Strategy_Annual_Report_2016.pdf (dostęp: 30.07.2020).
Raport Cert.gov.pl (dostęp: 27.05.2020).
Raport Europejskiej Komisji Praw Człowieka z 04.03.1994 r.
Raport Europol SOCTA 2017 r., *European Union serious and organised crime. Threat assessment* (dostęp: 27.05.2020).
Raport Komisji z dnia 20.05.1997 r.
Raport NIK https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/ (dostęp: 29.06.2020).
Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 r., http://cert.gov.pl (dostęp: 27.05.2019).
Raport RFN dla ONZ dok. nr S/AC.37/2003/(1455)/10.
Raport roczny za 2018 r., http://kaspersky.pl
Raport TE-SAT 2018–19, European Union Terrorism Situation and Trend Report 2019–2019 (dostęp: 30.06.2020).
Raport z postępów działań w ramach cyberstrategii 2016–2021 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/805677/National_Cyber_Security_Strategy_Progress_Report.pdf (dostęp: 30.07.2020).

Raport z postępów działań w ramach cyberstrategii 2016–2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/805677/National_Cyber_Security_Strategy_Progress_Report.pdf (dostęp: 30.07.2020).
Raport z realizacji cyberpolityki UK na lata 2011–2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_C.
Raport: Europol in brief 2018..
Report on Europe and the global information society. Interim report on trans-European networks Progress report on employment Extracts of the conclusions of the Presidency of the Corfu European, Council, Biulletiun of EU, Suppement 2/94.
Report on the Implementation of the European Security Strategy, dok. S407/08, Bruksela 11 grudnia 2008 <https://www.consilium.europa.eu/uedocs/.../reports/104630.pdf > (dostęp:13.08.2018).
http://www.apwg.org (dostęp: 27.05.2019)
http://www.cap.uni-muenchen.de/download/2004/2004_Venusberg_Report.pdf.
http://www.coe.int/cybercrime (dostęp: 11.07.2017).
https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpiecze%C5%84stwo-A.D.-2018.pdf.
https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalitaet-im-engeren-sinne-in-deutschland/ (dostęp: 23.07.2020).
https://www.economie.gouv.fr/files/files/directions_services/cge/Rapports/2017_02_CGE_SR_Rapport.pdf (dostęp: 30.07.2020).
https://www.europol.europa.eu/ec3 (dostęp:17.07.2020).
https://www.ons.gov.uk/ (dostęp: 15.08.2020).
www.livreblancdedefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf (dostęp: 30.08.2020).

Literatura

Abrahms M., *What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy*, „International Security" 2008, nr 32.

Adamczuk M., Liedel K., *Doktryna cyberbezpieczeństwa RP*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12.
Adamska M. (red.), *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, Warszawa, 2013.
Adamski A., *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005, nr 4(167).
Adamski A., *Cyberprzestępczość – rozwój regulacji prawnej w Europie. Doświadczenia krajowe na tle implementacji prawnych instrumentów zwalczania cyberprzestępczości*, „Prokuratura i Prawo" 2011, nr 6.
Adamski A., *Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę*, w: G. Szpor (red.), *Internet ochrona wolności własności i bezpieczeństwa*, Warszawa 2011.
Adamski D., *Europejskie prawo łączności elektronicznej – telefonia, telewizja, Internet*, Warszawa 2005.
Albahar M., *Cyber Attacks and Terrorism: A Twenty-First Century Conundrum*, „Sci Eng Ethics" 2019, nr 25(4).
Aleksandrowicz T.R., *Podstawy walki informacyjnej*, Warszawa 2016.
Aleksandrowicz T.R., *Strategia bezpieczeństwa narodowego Polski*, Warszawa 2013.
Aleksandrowicz T.R., *Terroryzm międzynarodowy*, Warszawa 2008.
Aleksandrowicz T.R., *Sieciowy paradygmat bezpieczeństwa państwa w stosunkach międzynarodowych*, Warszawa 2013.
Aleksandrowicz T.R., Liedel K., *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia*, w: K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, Warszawa 2014.
Andersson J., Biscop S., Giegerich B., Mölling Ch., Tardy T., *Envisioning European Defence: Five Futures*, „Chaillot Paper" 2017, nr 137.
Andrzejewska A., *Cyberświat – możliwości i zagrożenia*, Warszawa 2009.
Awan I., *Paving the Way for Extremism: How Preventing the Symptoms Does Not Cure the Disease of Terrorism*, „Journal of Terrorism Research" 2011, vol. 2(3).
Avbelj M., *Brexit: An End to the End of History*, „German Law Journal" 2016, vol. 17.

Aycock J., *Computer Viruses and Malware*, Calagary 2006.
Balawajder G., *Instytucjonalny wymiar ochrony granic zewnętrznych Unii Europejskiej w kontekście bezpieczeństwa państw członkowskich*, „Pogranicze. Polish Borderlands Studies" 2018, vol. 6(1).
Barber B., *Democracy and terror in the era of jihad vs. Mcworld*, w: K. Booth, T. Dunne (red.), *World in Collision: Terror and the Future of Global Order*, New York 2002.
Barcz J., *Przewodnik po Traktacie z Lizbony. Traktaty ustanawiające Unię Europejską*, Warszawa 2008.
Barcz J. (red.), *Prawo Unii Europejskiej. Zagadnienia systemowe*, Warszawa 2002.
Barcz J. (red.), *Traktat reformujący Unię Europejską,* „Koźmiński Law School Papers" 2007, nr 5.
Barcz J. (red.), *Traktat z Lizbony. Główne reformy ustrojowe Unii Europejskiej*, Warszawa 2008.
Barcz J., Kawecka-Wyrzykowska E., Michałowska-Gorywoda K., *Integracja europejska w okresie przemian,* Warszawa 2016.
Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Warszawa 2011.
Barrett D., King T., *Computer Networking Illuminated*, USA 2005.
Batorowska H., Motylińska P., *Bezpieczeństwo informacyjne i medialne w czasach nadprodukcji informacji*, Warszawa 2020.
Baylis J., *Bezpieczeństwo międzynarodowe i globalne w epoce pozimnowojennej*, w: *Globalizacja polityki światowej. Wprowadzenie do stosunków międzynarodowych*, Kraków 2008.
Bączek P., *Zagrożenie informacyjne*, Toruń 2005.
Bączek P., *Zagrożenia informacyjne a bezpieczeństwo Państwa Polskiego*, Toruń 2006.
Beaufre A., *Wstęp do strategii. Odstraszanie i strategia*, Warszawa 1968.
Becla A., *Społeczeństwo informacyjne i społeczeństwo pseudoinformacyjne – problemy pojęciowe i metodyczne identyfikacji*, „Handel Wewnętrzny" 2012, t. 3.
Berger P., Luckman T., *The Social Construction of Reality. A Treatise in the Sociology of Knowledge*, New York 1966.

Berlin A., Brotherson L., *Bezpieczeństwo defensywne. Podstawy i najlepsze praktyki*, Gliwice 2018.
Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Warszawa 2011.
Bieniek B., *Pranie pieniędzy w prawie międzynarodowym, europejskim oraz polskim*, Warszawa 2010.
Bierzanek R., *Współczesne stosunki międzynarodowe*, Warszawa 1972.
Biscop S., *The EU Global Strategy 2020*, „Security Policy Brief" 2019, nr 108.
Black J., Hall A., Cox K., Kepe M., Silfversten E., *Defence and security after Brexit. Understanding the possible implications of the UK's decision to leave the EU*, Santa Monica 2017.
Bohaczewski M., *Jurysdykcja krajowa w sprawie o naruszenie praw własności intelektualnej w internecie na tle orzecznictwa francuskiego*, w: A. Sztoldman (red.), *Prawo wobec innowacji technologicznych*, Warszawa 2013.
Bolechów B., *Terroryzm w świecie podwubiegunowym. Przewartościowania i kontynuacje*, Toruń 2002.
Boratyńska K., Górski A., Gruszczak A., Grzelak A., Hofmański P., Jasiński F., Kula M., Lach A., Nita B., Rakowska P., Sakowicz A., Sołtysińska A., Srebro B., *Zwalczanie przestępczości w Unii Europejskiej. Współpraca sądowa i policyjna w sprawach karnych*, Warszawa 2006.
Borkowski P.J., *Polityczne teorie integracji międzynarodowej*, Warszawa 2007.
Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.
Braun H., *The non-military threat spectrum*, „SIPRI Yearbook Oxford University Press", London 2003.
Brennan J., *The Impact on Counterterrorism*, Harvard 2005.
Bryksy P., Wy*brane zagadnienia polityki bezpieczeństwa wewnętrznego Unii Europejskiej. Szanse i zagrożenia dla Polski*, „Biuro Bezpieczeństwa Narodowego", Warszawa 2008.
Brzeziński D., *Wolność i bezpieczeństwo w płynnej nowoczesności*, „Studia Socjologiczno-Polityczne" 2017, vol. 6(1).

Brzeziński M., *Podnoszenie poziomu ochrony obywateli i przedsiębiorstw w cyberprzestrzeni*, w: W. Fehler, K.P. Marczuk (red.), *Polityka Unii Europejskiej w zakresie bezpieczeństwa wewnętrznego*, Warszawa 2015.
Brzeziński Z., *O Polsce, Europie i świecie 1988–2001*, Warszawa 2002.
Buregwa-Czuma S., Garwol K., *Definicje, właściwości i funkcje społeczeństwa informacyjnego*, „Dydaktyka Informatyki" 2011, nr 6.
Bures O., Carrapico H. (red.), *Security Privatization. How Non-security-related Private Businesses Shape Security Governance*, Warszawa 2018.
Buzan B., Waever O., de Wilde J., *Security: A New Framework for Analysis*, Colorado 1998.
Cała-Wacinkiewicz E., Menkes J., Nowakowska-Małusecka J., Przyborowska-Klimczak A., Staszewski W., *System Narodów Zjednoczonych z polskiej perspektywy*, Warszawa 2018.
Carrapico H., Barrinha A., *The EU as coherent (cyber) security actor?*, „Journal of Common Market Studies" 2017, vol. 55(6).
Castells M., *Społeczeństwo sieci*, Warszawa 2010.
Catelan N., Cimamonti S., Perrier J.B., *La luttecontre le terrorismedans le droit et la jurisprudence de l'Unioneuropeenne*, Marseille 2014.
Cesarz Z., Stadtmüller E., *Problemy polityczne współczesnego świata*, Wrocław 1996.
Chalk P., Rosenau W., *Confronting the Enemy Within*, Santa Monica 2004.
Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015.
Chapple M., Seidl D., *Cyberwarfare: Information Operations in a Connected World*, Burlington 2015.
Charyton A., *Wpływ Internetu na funkcjonowanie nastolatków*, w: R. Skubisz R. (red.), *Internet 2000. Prawo – ekonomia – kultura*, Lublin 2000.
Ching J., *Cyberterrorism*, New York 2010.
Christensen K., Liebetrau T., *A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry*, „Intelligence and National Security" 2019, vol. 34(3).

Ciecierski M., *Wywiad biznesowy w korporacjach transnarodowych. Teoria i praktyka,* Toruń 2009.
Ciechomska M., *Zmiana Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych szansą na powstanie globalnego instrumentu ochrony danych*, „Monitor Prawniczy" 2017, nr 25(16).
Cieślarczyk M., *Kultura bezpieczeństwa i obronności*, Siedlce 2006.
Cornwall H., *Datatheft. Computer Fraud, Industrial, Espionage and Information Crime*, London 1990.
Craig P., de Burca G., *EU Law. Text, Cases and Materials*, Oxford 2003.
Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami. Analiza sytuacji i rekomendacje działań, „Cyfrowa Polska", Warszawa 2019.
Cygan M., Geilke M., *Tworzenie systemu zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001:2014*, Wrocław 2015.
Czaja J., *Kulturowy wymiar bezpieczeństwa*. *Aspekty teoretyczne i praktyczne*, Kraków 2013.
Czapliński W., *Układy z Schengen jako przykład nowych form współpracy państw członkowskich UE*, w: B. Góralczyk (red.), *Polska Policja na drodze do Unii Europejskiej*, Warszawa 2000.
Czapliński W., *Układy z Schengen jako przykład nowych form współpracy państw członkowskich UE*, w: M. Boguszewski (red.), *Polska Policja na drodze do Unii Europejskiej*, Warszawa 2007.
Czapliński W., *Wprowadzenie do prawa Unii i Wspólnot*, Kraków 2002.
Czapliński W., Mik C., *Traktat o Unii Europejskiej. Komentarz*, Warszawa 2005, t. I.
Czaputowicz J., *Bezpieczeństwo w teoriach stosunków międzynarodowych*, Warszawa 2007.
Czaputowicz J., *Kryteria bezpieczeństwa międzynarodowego państwa – aspekty teoretyczne*, w: *Kryteria bezpieczeństwa międzynarodowego państwa*, Warszawa 2003.
Czaputowicz J., *System czy nieład? Bezpieczeństwo europejskie u progu XXI wieku*, Warszawa 1998.
Czosseck C., Ottis R., Talihärm A., *Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber*

Security, „International Journal of Cyber Warfare and Terrorism" 2011, vol. 1(1).
Czebotar Ł., *Strategia Stanów Zjednoczonych wobec problemu bezpieczeństwa cyberprzestrzeni*, w: A. Podraza, P. Potakowski, K. Wiak (red.), *Cyberterroryzm zagrożeniem XXI wieku*, Warszawa 2013.
Czyżak M., *Cyberprzestępczość a rozwój społeczeństwa informacyjnego*, „Ekonomiczne Problemy Usług" 2015, nr 117.
Daniluk P., *Kultura strategiczna Unii Europejskiej. Podejście normatywne*, „Rocznik Bezpieczeństwa Międzynarodowego" 2015, t. 9(2).
Dawidczyk A., *Nowe wyzwania, zagrożenia i szanse dla bezpieczeństwa Polski u progu XXI wieku*, Warszawa 2001.
Dąbrowska-Kardas M., Kardas P., *Przestępstwa przeciwko mieniu*, Kraków 1999.
Wilde P. de, Leupold A., Schmidtke H., *Introduction: The Differentiated Politicisation of European Governance*, „West European Politics" 2016, vol. 39(1).
Dela P., *Teoria walki w cyberprzestrzeni*, Warszawa 2020.
Dela P., *Zasady sztuki wojennej w cyberprzestrzeni*, w: A. Polak, J. Lasota, M. Palczewska (red.), *Wojny i konflikty zbrojne XXI wieku – podejście polemologiczne*, Warszawa 2016.
Denning D., *Cyberterrorism*, „Global Dialogue" Autumn 2000.
Depa M., Pomykała M., *Instytucjonalne aspekty przeciwdziałania cyberprzestępczości*, w: I. Oleksiewicz, M. Polinceusz, M. Pomykała (red.), *Nowoczesne technologie – źródło zagrożeń i narzędzie ochrony bezpieczeństwa*, Rzeszów 2014.
Domenach J., *Europa: wyzwanie dla kultury*, Warszawa 1992.
Drozd A., *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2007.
Dubisz S. (red.), *Uniwersalny słownik języka polskiego*, t. V, Warszawa 2003.
Dudka K. (red.), *Kodeks postępowania karnego. Komentarz*, Warszawa 2018.
Dunaj B. (red.), *Słownik współczesnego języka polskiego*, t. I, Warszawa 1999.

Encyklopedia PWN, t. 12, Warszawa 2010.
Fehler W., *O pojęciu bezpieczeństwa informacyjnego*, w: M. Kubiak, S. Topolewski (red.), *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce–Warszawa 2006.
Ficoń K., *Bezpieczeństwo*, Warszawa 2013.
Fijałkowska B., Żukowski A., *Unifikacja i zróżnicowanie się współczesnej Europy*, Warszawa 2002.
Fischer B., *Przestępstwa komputerowe i ochrona informacji*, Kraków 2000.
Frączek M., *Bezpieczeństwo cyberprzestrzeni państwa – podstawowe problemy*, w: A. Polak, J. Lasota, M. Palczewska (red.), *Wojny i konflikty zbrojne XXI wieku – podejście polemologiczne*, Warszawa 2016.
Fukuyama F., *Their target: The Modern Word*, „Newsweek" 17.12.2001.
Gajda A.*, Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomiczno-Społecznego Studia i Prace. Szkoła Główna Handlowa" 2014, nr 4.
Galewski T., *Transformacja społeczna w kierunku społeczeństwa informacyjnego: wizja czy rzeczywistość?*, „Zeszyty Naukowe Wyższej Szkoły Bankowej", Wrocław 2011, nr 22.
Galloway F., *Anti-Terrorism Resolutions: The Security Council's Threat to the UN System*, „Journal of Terrorism Research" 2011, vol. 2(3).
Garrison Ch., Hamilton C., *A comparative analysis of the EU GDPR to the US's breach notifications*, „Information & Communications Technology Law" 2019, vol. 28(1).
Gibson W., *Neuromancer*, Warszawa 2001.
Gienas K., *Systemy Digital Rights Management w świetle prawa autorskiego*, Warszawa 2008.
Giezek J. (red.), *Kodeks karny. Komentarz*, Warszawa 2007.
Gizicki W., *Polityczne uwarunkowania bezpieczeństwa europejskiego*, Toruń 2008.
Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Warszawa 1999.
Golinowski J., *Perspektywa porządku postpolitycznego. W stronę technologii władzy*, Warszawa 2007.

Golka M., *Bariery w komunikowaniu i społeczeństwo dezinformacyjne*, Warszawa 2008.
Golonka A., *Cyberprzestępczość – międzynarodowe standardy zwalczania zjawiska a polskie regulacje prawne*, „Studia Prawnicze. Rozprawy i Materiały" 2016, nr 1(18).
Góral R., *Kodeks karny. Komentarz praktyczny*, Warszawa 2007.
Górka M., *Istota bezpieczeństwa cybernetycznego w polityce państw Grupy Wyszehradzkiej w latach 2013–2017*, Toruń 2019.
Górka M. (red.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa XXI wieku*, Warszawa 2014.
Górniok O., *Kodeks karny. Komentarz*, Gdańsk 2008.
Grajny M., *The European Union Counterterrorism Policy Before and After the 9/11 Attacks: To Extend What Does EU Have an Integrated Policy Towards Terrorism*, Kraków 2008.
Graś A., *Konwencja z Prüm – pozytywne i negatywne konsekwencje*, „Biuletyn Analiz UKIE" 2006, nr 16.
Graś A., *Porozumienie z Schengen – geneza i stan obecny*, w: P. Jaworski (red.), *Polska droga do Schengen. Opinie ekspertów*, Warszawa 2001.
Gruszczak A., *Eurojust i jego miejsce w europejskiej współpracy sądowej,* „Państwo i Prawo" 2003, nr 4.
Gruszczak A., *III filar Unii Europejskiej po Tampere: wnioski i perspektywy*, „Studia Europejskie" 2000, nr 3.
Gruszczak A., *Unia Europejska wobec przestępczości*, Kraków 2002.
Gruszczak A., *Wzmocniona współpraca w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych Unii Europejskiej*, „Studia Europejskie" 2002, nr 2.
Gryz J., *Bezpieczeństwo państwa władza – polityka – strategia*, Warszawa 2013.
Gryz J., *Paradygmaty bezpieczeństwa*, w: P. Sienkiewicz, M. Marszałek, H. Świeboda (red.), *Metodologia badań bezpieczeństwa narodowego*, t. II, Warszawa 2011.
Gryz J., *Wzajemny związek między polityką i strategią a bezpieczeństwem państwa*, „Rocznik Bezpieczeństwa Międzynarodowego" 2007, nr 2.

Gryz J. (red.), *Strategia bezpieczeństwa narodowego Polski*, Warszawa 2013.
Gryz J. (red.), *Zarys teorii bezpieczeństwa państwa*, Warszawa 2016.
Grzelak A., *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości. W stronę standardu europejskiego*, Warszawa 2015.
Grzelak A., *Traktat formujący UE – proponowane zmiany w dziedzinie Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości UE,* w: J. Barcz J. (red.), *Traktat reformujący Unię Europejską*, „Koźmiński Law School Papers" 2007, nr 5.
Grzelak A., *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości*. *Komentarz*, Warszawa 2019.
Grzelak A., Królikowski M., Sakowicz A. (red.), *Europejskie prawo karne 2012*, Warszawa 2012.
Gulda P., *Internet a prawa człowieka*, „Gdańskie Studia Prawnicze" 2005, nr 13.
Guzik-Makaruk E.M., *Regulacje prawne przewidziane w prawie policyjnym*, w: E.W. Pływaczewski (red.), *Przestępczość zorganizowana*, Warszawa 2011.
Haataja S., *The 2007 Cyberattacks Against Estonia and International Law on the Use of Force: An Informational Approach*, „Law, Innovation and Technology" 2017, vol. 9.
Haliżak E., Kuźniar E., Michałowska G., Parzymies S., Simonides J., Zięba R. (red.), *Stosunki międzynarodowe w XXI wieku. Księga jubileuszowa z okazji 30-lecia Instytutu Stosunków Międzynarodowych Uniwersytetu Warszawskiego*, Warszawa 2006.
Harrel Y., *Rosyjska cyberstrategia*, Warszawa 2015.
Hoffman B., *Is Europe Soft on Terrorism?*, „Foreign Policy" 1999, nr 115.
Hollis D., *Cyberwar Case Study*: *Georgia 2008*, „Small Wars Journal" 2011.
Hołyst B., *Bezpieczeństwo. Ogólne problemy badawcz*e, Warszawa 2014.
Hołyst B., *Bezpieczeństwo społeczeństwa*, Warszawa 2015.
Hołyst B., *Terroryzm*, Warszawa 2011.

Huntington S.P., *Zderzenie cywilizacji i nowy kształt ładu światowego*, Poznań 2018.
Indecki K., *Prawo karne wobec terroryzmu i aktu terrorystycznego*, Łódź 1998.
Ilves L.K., Evans T.J., Cilluffo F.J., Nadeau A.A., *European Union and NATO Global Cybersecurity Challenges: A Way Forward*, „Prism: A Journal of the Center for Complex Operations" 2016, vol. 6(2).
Jałoszyński K., *Współczesny wymiar antyterroryzmu*, Warszawa 2008.
Jałoszyński K., Aleksandrowicz T., Wiciak K., *Bezpieczeństwo państwa a zagrożenie terroryzmem. Instytucje państwa wobec zagrożenia terroryzmem*, t. II, Szczytno 2016.
Janczak J., Nowak A., *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013.
Janczak J., Świdzikowski G., *Bezpieczeństwo informacji w woskowym systemie telekomunikacyjnym*, Warszawa 2004.
Janowski J., *Cybernetyzacja prawa*, w: E. Galewska, S. Kotecka (red.), *X-lecie CBKE. Księga pamiątkowa z okazji 10-lecia Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego*, Warszawa 2012.
Janowski M., *Przestępstwo tzw. oszustwa komputerowego*, „Prokuratura i Prawo" 2011, nr 10.
Jarmoszko S., *Antropologia bezpieczeństwa. Kontury naukowej tożsamości*, Siedlce 2015.
Jarmoszko S., *Bezpieczeństwo kulturowe i kultura bezpieczeństwa jako kategorie antropologiczne*, w: P. Żarkowski, S. Tobolewski (red.), *Współczesne bezpieczeństwo kulturowe*, Siedlce 2014.
Jaroszewska A., *Wybrane aspekty cyberprzestępczości w cyberprzestrzeni. Studium prawno-karne i kryminologiczne*, Olsztyn 2017.
Jasiński F., Narojek M., Rakowski P., *Strategia antyterrorystyczna Unii Europejskiej*, „Wspólnoty Europejskie" 2006, nr 1.
Jasiński F., Rakowski P., *Unia Europejska wobec walki z terroryzmem*, w: A. Górski, A. Sakowicz (red.), *Zwalczanie przestępczości w Unii Europejskiej. Współpraca sądowa i policyjna w sprawach karnych*, Warszawa 2006.
Jaskuła S., *Informacyjna przestrzeń tożsamości*, Warszawa 2010.

Jasudowicz T., *Ochrona danych osobowych. Standardy europejskie. Zbiór materiałów*, Toruń 1998.
Jean C., *Geopolityka*, Wrocław 2002.
Jemioło T., Dawidczyk A., *Wprowadzenie do metodologii badań bezpieczeństwa*, Warszawa 2008.
Kamiński M., *System cyberbezpieczeństwa Republiki Estonii. Czy warto wzorować się na estońskich rozwiązaniach prawno-organizacyjnych?*, w: W. Kitler, K. Chałbińska-Jentkiewicz, K. Badzimirowska-Masłowska (red.), *System bezpieczeństwa w cyberprzestrzeni RP*, Warszawa 2018.
Kamiński M., *Ujednolicenie prawa w zakresie systemowych rozwiązań ochrony ludności i obrony cywilnej*, w: J. Gawęcka, J. Wojtycza (red.), *Współczesna obrona cywilna. Wyzwania, ryzyko, zagrożenia*, Piotrków Trybunalski 2018.
Kamiński M., Strużewska-Smirnow J., Wieczerza M., *Charakterystyka modeli systemów bezpieczeństwa teleinformatycznego oraz ochrony sieci teleinformatycznych z punktu widzenia służb specjalnych*, w: P. Pogonowski (red.), *Charakterystyka modeli systemów bezpieczeństwa teleinformatycznego oraz ochrony sieci teleinformatycznych z punktu widzenia służb specjalnych*, Warszawa 2017.
Kańciak A., *Unia Europejska na drodze do zwiększenia ochrony cyberprzestrzeni. Wybrane zagadnienia prawne*, „Studia Prawnoustrojowe" 2017, nr 38.
Kapica W. (red.), *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa 2020.
Kardas P., *Prawnokarna ochrona informacji z perspektywy przestępstw komputerowych*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, t. 4(1).
Karnouskos S., *Stuxnet Worm Impact on Industrial Cyber–Physical System Security*, w: *37th Annual Conference of the IEEE Industrial Electronics Society*, Melbourne 2011.
Karpiuk M., Prokop K., *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne,* Olsztyn 2016.

Kasowska-Pedrycz K., *Polityka bezpieczeństwa wewnętrznego UE – ewolucja i perspektywy*, w: R. Bäcker, J. Marszałek-Kawa, J. Modrzyńska (red.), *Od starej do nowej Europy?*, Toruń 2005.
Kądziołka K., *Ocena poziomu zagrożenia terroryzmem w krajach Unii Europejskiej z wykorzystaniem GTI*, „Ekonomia Międzynarodowa" 2018, nr 2.
Kitler W., Taczkowska-Olszewska J., Radoniewicz F., *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.
Kjærgaard-Christensen K., Liebetrau T., *A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry*, „Intelligence and National Security" 2019, vol. 34(3).
Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych*, wyd. 18, Warszawa 1989.
Kopczewski M.*, Elementy infrastruktury krytycznej państwa, organizacji jako obiekty narażone na ataki cyberterrorystyczne*, Zakopane 2011.
Korczyński R., Koszut R., *„Oszustwo" komputerowe*, „Prokuratura i Prawo" 2002, nr 2.
Korczyk H., *Bezpieczeństwo i rozbrojenie w projektach Ligi Narodów,* „Mazowieckie Studia Humanistyczne" 2005, nr 1–2.
Kosiński J., *Działania terrorystyczne a cyberprzestępczość*, w: J. Szafrański, J. Kosiński (red.), *Współczesne zagrożenia terrorystyczne oraz metody ich zwalczania. Materiały pokonferencyjne*, Szczytno 2007.
Kostecki W., *Analiza czynnikowa stosunków międzynarodowych*, Warszawa 2015.
Kowalkowski S. (red.), *Niemilitarne zagrożenia bezpieczeństwa publicznego*, Warszawa 2011.
Kowalski D., Kwiatkowski M., Zduniak A. (red.), *Edukacja dla bezpieczeństwa – wybrane perspektywy*, Lublin–Poznań 2004.
Kozłowski A., *Bezpieczeństwo cybernetyczne w strategicznych dokumentach Wielkiej Brytanii 2009–2011*, w: I. Panier (red.), *Wielka Brytania i Wspólnota u progu XXI wieku. Przeszłość – teraźniejszość – perspektywy*, Łódź 2014.

Kruk A.M., *Bezpieczeństwo transferu informacji w XXI wieku w świetle bezpieczeństwa państwa i organizacji*, w: S. Sulowski, M. Brzeziński (red.), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Warszawa 2009.
Krysiński Ł., *Identyfikacja cyberprzestępców*, „Państwo i Prawo" 2020, nr 2.
Krztoń W., *Walka o informację w cyberprzestrzeni w XXI wieku*, Warszawa 2017.
Krztoń W., Oleksiewicz I., *Bezpieczeństwo współczesnego społeczeństwa informacyjnego w cyberprzestrzeni*, Warszawa 2017.
Kubin J., *Projektowanie strategii*, w: J. Kubin, Z. Żekoński (red.), *W poszukiwaniu strategii zmian*, Warszawa 1993.
Kuhn T.S., *Raz jeszcze o paradygmatach*, w: T.S. Kuhn (red.), *Dwa bieguny. Tradycja i nowatorstwo w badaniach naukowych*, Warszawa 1985.
Kuhn T.S., *Struktura rewolucji naukowych,* Warszawa 2001.
Kukułka J. (red.), *Bezpieczeństwo a współpraca europejska: współzależności i sprzeczności interesów*, „Sprawy Międzynarodowe" 1982, nr 7.
Kukułka J., *Bezpieczeństwo międzynarodowe w Europie Środkowej po zimnej wojnie*, Warszawa 1994.
Kukułka J., *Międzynarodowe stosunki polityczne*, Warszawa 1982.
Kula M., Lach A., Nita B., Rakowska P., Sakowicz A., Sołtysińska A., Srebro B., *Zwalczanie przestępczości w Unii Europejskiej. Współpraca sądowa i policyjna w sprawach karnych*, Warszawa 2006.
Kulesza J., *Międzynarodowe prawo Internetu*, Poznań 2010.
Kunikowski J., *Wiedza i edukacja dla bezpieczeństwa*, Warszawa 2002.
Kupiecki R., *Strategia Bezpieczeństwa Narodowego RP 2014 jako instrument polityki państwa. Uwarunkowania zewnętrzne i aspekty procesowe*, „Bezpieczeństwo Narodowe" 2015, nr 1.
Kupiecki R., *Kultura strategiczna podmiotów zbiorowych. Przypadek NATO*, „Sprawy Międzynarodowe" 2017, nr 4.
Kuźniar R., *Europejska strategia bezpieczeństwa,* „Polska w Europie" 2004, nr 2(46).
Kuźniar R., *Między polityką a strategią*, Warszawa 1994.

Kwećka R., *Strategia bezpieczeństwa informacyjnego państwa*, Warszawa 2014.
Kwećka R., *Zarys teorii bezpieczeństwa informacyjnego państwa*, w: J. Gryz (red.), *Zarys bezpieczeństwa państwa*, Warszawa 2016.
Lach A., *Kradzież tożsamości*, „Państwo i Prawo" 2012, nr 3.
Lakatos I., Musgrave A. (red.), *Criticism and the Growth of Knowledge*, Cambridge 1999.
Lakomy M., *Unia Europejska wobec zagrożeń dla bezpieczeństwa teleinformatycznego – zarys problemu*, „Rocznik Integracji Europejskiej" 2013, nr 7.
Lem S., *Bomba megabitowa*, Kraków 1999.
Lankosz K. (red.), *Traktat o Unii Europejskiej – komentarz*, Warszawa 2003.
Lankosz K., Chrościcki M., Czubik P. (red.), *Walka z terroryzmem międzynarodowym w świetle prawa międzynarodowego*, Bielsko-Biała 2004.
Lankosz K. (red.), Szczygieł M., *Polityka cyberbezpieczeństwa Unii Europejskiej – początek drogi do strategicznej autonomii*, „Sprawy Międzynarodowe" 2018, nr 2.
Lepa A., *Świat manipulacji*, Częstochowa 1995.
Lewandowski K., *Przestępstwa przeciwko ochronie informacji w świetle Rozdziału XXXIII kodeksu karnego, orzecznictwa i doktryny*, „Wojskowy Przegląd Prawniczy" 2010, nr 3.
Lasota A., *Cyberatak jako wstęp do cyberwojny*, „Studia Mazowieckie" 2014, nr 4.
Lévy P., *Drugi potop*, w: M. Hopfinger (red.), *Nowe media w komunikacji społecznej w XX wieku*, Warszawa 2002.
Lichocki E., *Cyberterroryzm jako nowa forma zagrożeń dla bezpieczeństwa*, w: K. Liedel (red.), *Transsektorowe obszary bezpieczeństwa Narodowego*, Warszawa 2011.
Lichocki E., Mirosław T., *Bezpieczeństwo Sił Zbrojnych RP w dobie zagrożeń cybernetycznych*, w: K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w dobie informacji*, Warszawa 2014.
Liddell B.H., *Strategia działań pośrednich*, Warszawa 1959.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008.
Liedel K., Piasecka P., *Terroryzm wczoraj i dziś*, Warszawa 2015.
Liedel K., Piasecka P., *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 1.
Liedel K., Serafin T., *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011.
Lindley-French J., Algieri F., *A European Defence Strategy*, Güetersloh 2004.
Littlejohn Shinder D., Tittel E., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Gliwice 2004.
Loiseau H., Lemay L., *Canada's Cyber Security Policy: A Tortuous Path Toward a Cyber Security Strategy*, w: D. Ventre (red.), *Cyber Conflict. Competing National Perspectives*, London 2012.
Loranty K., *Bezpieczeństwo społeczne RP*, Warszawa 2004.
Lup Jr J.R., *Eschatology in a Secular Age: An Examination of the Use of Eschatology in the Philosophies of Heidegger, Berdyaev and Blumenberg*, Florida 2013.
Łapczyński M., *Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*, „Pułaski Policy Papers" 2009, nr 7.
Łepkowski W., *Podstawy strategii wojskowej*, Warszawa 2006.
Łuczak J. (red.), *Zarządzanie bezpieczeństwem informacji*, Poznań 2004.
Madej M., *Instytucjonalizacja współpracy międzynarodowej w dziedzinie zwalczania terroryzmu w Europie*, w: S. Parzymies, R. Zięba (red.), *Instytucjonalizacja wielostronnej współpracy międzynarodowej w Europie*, Warszawa 2004.
Malešević S., *Terrorism. In The Rise of Organised Brutality: A Historical Sociology of Violence*, Cambridge 2017.
Malinowski M., Ożarowski R., Grabowski W., *Ewolucja terroryzmu na przełomie XX i XXI wieku*, Gdańsk 2009.
Manzano M., *Cyberwarfare*, Singapur 2018.
Marczyk M., *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, „Przegląd Teleinformatyczny" 2018, nr 1–2.
Marek A., *Kodeks karny. Komentarz*, Warszawa 2010.

Markowski A., *Nowy słownik poprawnej polszczyzny*, Warszawa 1999.
Masuda Y., *The information society as post-indrustial society*, Waszyngton 1983.
Matysiak A., Struś M., *Paradygmat rozwoju zrównoważonego*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2015, nr 213.
Mazurkiewicz A., *NATO and EU approach towards civil-military relations in militaryoperations*, „Polityka i Społeczeństwo" 2014, nr 2.
McLeish C., *Recasting the Threat of Chemical Terrorism in the EU: The Issue of Returnees from the Syrian Conflict*, „European Journal of Risk Regulation" 2017, nr 8(4).
Michalski K., Oleksiewicz I., Sienkiewicz K., *Bezpieczeństwo online i offline*, Warszawa 2017.
Michniak J., *Bezpieczeństwo teleinformatyczne w zarządzaniu kryzysowym*, Warszawa 2004.
Mickiewicz P., *System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza,* „Rocznik Bezpieczeństwa Międzynarodowego" 2017, vol. 11(1).
Mickiewicz P., *System bezpieczeństwa narodowego w rozwiązaniach systemowych wybranych państw,* Warszawa 2018.
Milczarek E., *Współczesne wyzwania ochrony bezpieczeństwa informacyjnego jednostki w Internecie*, w: M. Porzeżyński, A. Borcuch (red.), *Bezpieczeństwo w erze społeczeństwa informacyjnego. Wyzwania w sferach kultury, marketingu i gospodarki*, Kielce 2019.
Milner H.V., *The Digital Divide – The role of political institutions in Technology Diffusion*, „Comparative Political Studies" 2006, vol. 39(2).
Młotek M., Siedlarz M., *Rządowy Zespół Reagowania na Incydenty Komputerowe. CERT.GOV.PL*, „Przegląd Bezpieczeństwa Wewnętrznego" 2011, nr 4.
Mockatis T.R., *The New Terrorism: Myths and Realists*, „Stanford University Press" 2008.
Moravcsik A., *Liberal International Relations Theory: A Scientific Assessment*, w: C. Elman, M. Fendius Elman (red.), *Progress in*

International Relations Theory: Appraising the Field, Cambridge 2003.
Moravcsik A., *Taking Preferences Seriously: A Liberal Theory of International Politics*, „International Organization" 2007, nr 4(51).
Mozgawa M., w: J. Warylewski (red.), *Przestępstwa przeciwko dobrom indywidualnym*, t. 10, Seria: *System Prawa Karnego*, Warszawa 2016.
Nanopoulos E., *The Fight against Terrorism, Fundamental Rights and the EU Courts: The Unsolved Conundrum*, „Cambridge Yearbook of European Legal Studies" 2012, nr 14.
Nazar K., *Glosa do postanowienia Sądu Najwyższego z dnia 12 grudnia 2013 r.*, „Prawo w Działaniu Sprawy Karne" 2016, nr 26.
Niedźwiecki A., *Paradygmat liberalny wobec problemu dezintegracji instytucji międzynarodowych,* „Przegląd Zachodni" 2019, nr 2.
Niżnik J., *Socjologia wiedzy*, Warszawa 1979.
Nosal C., *Psychologia myślenia i działania menedżera*, Kraków 2001.
Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011.
Nowak J.S., Bliźniuk G., *Społeczeństwo informacyjne: doświadczenie i przyszłość*, Katowice 2006.
Nowak L., *O ukrytej jedności nauk społecznych i nauk przyrodniczych*, http://www.staff.amu.edu.pl/~epistemo/Nowak/przyrhum.pdf (dostęp: 21.10.2009).
Nowakowski Z., Szafran H., Szafran R., *Strategia bezpieczeństwa narodowego Polski na tle strategii bezpieczeństwa wybranych państw*, Warszawa 2014.
Nowicki W., *Podstawy terminologii*, Warszawa 1986.
Oleksiewicz I., *Challenges of EU security on the example of cyberrorism policy*, „Journal of International Trade Law of Policy" 2015, nr 1.
Oleksiewicz I., *Cyberbezpieczeństwo i sztuczna inteligencja w sektorze energetycznym UE,* „Rocznik Bezpieczeństwa Międzynarodowego" 2020, t. 13, nr 1.
Oleksiewicz I., *Cyberterroryzm – jako przykład łamania prawa godności człowieka*, w: T. Jemioła, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm nowe wyzwania XXI wieku*, Warszawa 2009.
Oleksiewicz I., *Podstawy prawne współpracy karnej i policyjnej Unii Europejskiej w ramach polityki antyterrorystycznej Europejskiej*, w: I.

Oleksiewicz, M. Pomykała, J. Rajchel (red.), *Współpraca instytucjonalna w Unii*, Rzeszów 2010.
Oleksiewicz I., *Polityka antyterrorystyczna Unii Europejskiej*, Lublin 2013.
Oleksiewicz I., *Polska polityka antyterrorystyczna na tle standardów Unii Europejskiej*, „Przegląd Prawa Publicznego", Warszawa 2015, nr 6.
Oleksiewicz I., *Polskie prawo karne w zakresie walki z cyberprzestępczością na tle standardów prawa UE*, w: M. Pietraś, H. Chałupczak, J. Misiągiewicz (red.), *Europa Środkowo-Wschodnia w procesie transformacji i integracji. Wymiar bezpieczeństwa*, Zamość 2016.
Oleksiewicz I., *Uchodźcy w Unii Europejskiej. Aspekty prawne i polityczne*, Bydgoszcz–Rzeszów 2006.
Oleksiewicz I., *Ustawodawstwo polskie wobec przestępstwa o charakterze terrorystycznym*, w: Z. Nowakowski, J. Rajchel, H. Szafran, R. Szafra (red.), *Wspólna polityka bezpieczeństwa i obronności. Implikacja dla Polski*, Warszawa 2011.
Oleksiewicz I., *Zarys polityki cyberbezpieczeństwa Unii Europejskiej. Casusu Polski i RFN*, Warszawa 2019.
Oleksiewicz I., Górka M., *Bezpieczeństwo pozamilitarne i quasi-militarne Europy Zachodniej*, Toruń 2019.
Oleksiewicz I., Michalski K., Sienkiewicz E., *Bezpieczeństwo społeczeństwie informacyjnym. Zagadnienia w wymiarze on line i offline*, Warszawa 2017.
Oleksiewicz I., Polinceusz M., Pomykała M. (red.), *Nowoczesne technologie – źródło zagrożeń i narzędzie ochrony bezpieczeństwa*, Rzeszów 2014.
Oleksiewicz I., Stachurska-Szczesiak K., *Oszustwo komputerowe a polityka bezpieczeństwa informacyjnego Polski*, w: P. Bogdalski, Z. Nowakowski, T. Płusa, J. Rajchel, K. Rajchel (red.), *Współczesne zagrożenia cyberterrorystyczne i bioterrorystyczne a bezpieczeństwo narodowe Polski*, Warszawa–Dęblin 2015.
Oleksiewicz I., Zacharski R., Topolski I., *Faces of the Modern World. Political Dimension*, Berlin 2018.
Oleński J., *Ekonomika informacji. Metody*, Warszawa 2003.

Opitek P., *Skimming – aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej*, Warszawa 2017.
Oppermann K., *The Politics of Avoiding Referendums on the Treaty of Lisbon*, „Journal of European Integration" 2013, vol. 35(1).
Ottis R., *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, „Cooperative Cyber Defence Centre of Excellence", Tallinn 2008.
Pałka R., *Realizacja Strategii Lizbońskiej w latach 2000–2010 – zalecenia i rekomendacje, w tym dla Polski*, „Mazowsze. Studia Regionalne" 2011, nr 6.
Parzymies S., *Stan debaty na temat federalnego kształtu Unii Europejskiej,* w: J. Zając, A. Włodkowska-Bagan, M. Kaczmarski (red.), *Bezpieczeństwo międzynarodowe. Polska – Europa – Świat*, Warszawa 2015.
Pawłowski J. (red.), *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2002.
Paździor M., Trubalska J., *Pojęcie bezpieczeństwa państwa*, w: M. Paździor, J. Trubalska, Ł. Wojciechowski, A. Żywicka (red.), *Bezpieczeństwo państwa w XXI wieku*, Lublin 2018.
Piątek A., *Edukacja na rzecz bezpieczeństwa*, Warszawa 2011.
Pieczywok A., Loranty K. (red.), *Bezpieczeństwo jako problem edukacyjny*, Warszawa 2015.
Pietraś M., *Bezpieczeństwo międzynarodowe*, w: M. Pietraś (red.), *Międzynarodowe stosunki polityczne*, Lublin 2007.
Pietraś Z.J., *Podstawy teorii stosunków międzynarodowych*, Lublin 1986.
Pietraś Z.J., *Wyznaczniki polityki zagranicznej państwa*, w: A. Bodnar, J. Szczepański (red.), *Stosunki międzynarodowe. Problemy badań i teorii*, Warszawa 2007.
Pitts V., *Cyber Crimes: History of World's Worst Cyber Attacks*, Marousi 2017.
Płusa T., *Aktualne trendy w bioterroryzmie i w obronie przed nim*, w: P. Bogdalski, Z. Nowakowski, T. Płusa, J. Rajchel, K. Rajchel (red.), *Współczesne zagrożenia cyberterrorystyczne i bioterrorystyczne a bezpieczeństwo narodowe Polski*, Warszawa–Dęblin 2015, s. 407.
Pływaczewski E., *Kodeks karny. Komentarz*, Warszawa 2010.

Pokruszyński W., *Uwarunkowania współczesnego bezpieczeństwa międzynarodowego*, Szczytno 2006.
Pokruszyński W., *Bezpieczeństwo: teoria i praktyka*, Józefów 2012.
Pokruszyński W., *Etymologia polityki i strategii bezpieczeństwa w świetle wyzwań i zagrożeń XXI wieku*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje" 2018, nr 22.
Pokruszyński W., *Polityka a strategia bezpieczeństwa*, Józefów 2011.
Pokruszyński W., *Polityka Teoria – Bezpieczeństwo*, Józefów 2012.
Pokruszyński W., *Współczesne bezpieczeństwo narodowe*, Józefów 2009.
Polak E., *Od „ciężkiej" do wirtualnej gospodarki*, „Transformacje" 2010, nr 1–2.
Polinceusz M., Pomykała M., *Ochrona cyberbezpieczeństwa w Polsce. Kierunki zmian legislacyjnych na przestrzeni ostatnich lat*, w: P. Bogdalski, Z. Nowakowski, T. Płusa, J. Rajchel, K. Rajchel (red.), *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, Warszawa 2013.
Porębski A., *Europejskie mniejszości etniczne. Geneza i kierunki przemian*, Kraków 1991.
Powszechna encyklopedia filozofii, Lublin 2007.
Prokop K., *Ocena norm konstytucyjnych dla realizacji skutecznego systemu bezpieczeństwa narodowego, ze szczególnym uwzględnieniem stanu wojny. Ocena stanu obecnego i rekomendacje na przyszłość*, „Biuro Bezpieczeństwa Narodowego", Warszawa 2011.
Protasowicki I., Nowakowski Z., *Działania Unii Europejskiej na rzecz bezpieczeństwa informacyjnego*, Warszawa 2013.
Przesławski T., *Cel w konstrukcji przestępstwa terrorystycznego*, „Prokuratura i Prawo" 2009, nr 5.
Raczkowski K., Żukrowska K., Żuber M. (red.), *Interdyscyplinarność nauk o bezpieczeństwie. Paradygmat. Wiedza. Demarkacja*, Warszawa 2013.
Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.
Radoniewicz F., *Postanowienia decyzji ramowej Rady w sprawie ataków na systemy informatyczne a ujęcie cyberprzestępstw w*

kodeksie karnym, „Ius Novum" 2009, nr 1.
Rathmell A., *Information warfare and sub-state actors: An organizational approach,* „Information, Communication and Society" 1998, vol 1(4).
Rattray G.J., *Wojna strategiczna w cyberprzestrzeni,* Warszawa 2000.
Reginia-Zacharski J., Oleksiewicz I., Topolski I., *The faces of the modern Word. Political dimmention*, Berlin 2018.
Roberts A., *Counter – terrorism, armed force and the laws of war*, „Survival" 2002.
Rotfeld A.D., *Bezpieczeństwo międzynarodowe czasu przemian*, Warszawa 2004.
Sacewicz K., *Niemiecka strategia ochrony cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego", vol. 7(12).
Safjański T., *Prawne aspekty wykorzystania wsparcia Interpolu w poszukiwaniu osób podejrzanych w świetle art. 605a k.p.k.*, „Prokuratura i Prawo" 2016, nr 10.
Sakowicz A., *Prawnokarne gwarancje prywatności*, Łódź 2006.
Sawicki R., *Z orzecznictwa Europejskiego Trybunału Sprawiedliwości. Orzeczenie Sądu I Instancji z dnia 11 lutego 2003 r. w połączonych sprawach C–187/01 i C–385/01*, „Prokuratura i Prawo" 2005, nr 2.
Schreier F., *On cyberwarfare,* DCAF Horizon 2015, working paper.
Schütz P., *Zum Leben zu wenig, zum Sterben zu viel? Die finanzielle und personelle Ausstattung deutscher Datenschutzbehörden im Vergleich*, w: A. Roßnagel i wsp. (red.), *Die Zukunft des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung*, Wiesbaden 2018.
Shor E., *Constructing a Global Counterterrorist Legislation Database: Dilemmas, Procedures, and Preliminary Analyses*, „Journal of Terrorism Research" 2011, vol. 2(3).
Sieber U., *Cybercrime and Jurisdiction in Germany. The Present Situation and the Need for New Solutions*, w: B.J. Koops, S.W. Brenner (red.), *Cybercrime and Jurisdiction. A global survey*, „Information Technology & Law Series" 2006, vol. 11.
Sienkiewicz P., *Natura bezpieczeństwa w perspektywie systemowe*j, w: K. Drabik (red.), *Natura bezpieczeństwa w perspektywie personalnej i strukturalnej*, Warszawa 2013.

Sienkiewicz P., *Prognozowanie rozwoju globalnego społeczeństwa informacyjnego: wizje i scenariusze*, w: A. Szewczyk, E. Kot (red.), *Fenomen Internetu*, Szczecin 2008, t. I.
Sienkiewicz P., *Teoria rozwoju społeczeństwa informacyjnego*, Kraków 2004.
Sienkiewicz P., Świeboda H., *Społeczna percepcja zagrożeń bezpieczeństwa obywatelskiego*, Warszawa 2005.
Siudak R., *5G. Szanse, zagrożenia, wyzwania*, Kraków 2020.
Siwicki M., *Cyberprzestępczość*, Warszawa 2013.
Siwicki M., *Pojęcie locus delicti i zasady jurysdykcji karnej w ujęci prawno-porównawczym,* cz. 1, „Europejski Przegląd Sądowy" 2011, nr 9.
Skibiński F., *Rozważania o sztuce wojennej*, Warszawa 1972.
Skowera D., *Akademia Cyberpolicyjna – Policja i organizacje międzynarodowe wobec wyzwań przestępczości internetowej*, „Zarządzanie Publiczne" Zeszyty Naukowe ISP UJ 2006, nr 2.
Slater D., *Social Relationships and Identity Online and Offline*, w: L. Lievrouw, S. Livingston (red.), *The Handbook of New Media*, London 2002.
Smarzewski M., *Cyberterroryzm a cyberprzestępstwa o charakterze terrorystycznym*, „IUS NOVUM" 2017, nr 1.
Soja M., *Samorząd terytorialny w procesie integracji europejskiej. Polskie doświadczenia i wnioski na przyszłość*, Katowice 2008.
Soja M., *Stosunki UE – NATO w dziedzinie bezpieczeństwa europejskiego i obrony na przełomie XX i XXI wieku*, Warszawa 2011.
Soroka P., *Polistrategia bezpieczeństwa zewnętrznego Polski. Ujęcie normatywne*, Warszawa 2005.
Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996.
Steinmüller W., *Zautomatyzowane systemy informacyjne w administracji prywatnej i publicznej*, „Organizacja – Metoda – Technika" 1977, nr 9.
Stronikowska G., *Prokuratura europejska jako instytucja ochrony interesów finansowych Unii Europejskiej*, Warszawa 2020.
Strużewska-Smirnow J., Wieczerza M., *Ustawowe uprawnienia operacyjno-rozpoznawcze i dochodzeniowo-śledcze służb specjalnych w zakresie wykrywania zagrożeń bezpieczeństwa narodowego w*

systemach i sieciach teleinformatycznych z perspektywy międzynarodowej, w: P. Pogonowski (red.), *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego: wybrane zagadnienia*, Warszawa 2017.
Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.
Sulowski S., *Państwo i bezpieczeństwo w kazualnym związku,* w: S. Sulowski, M. Brzeziński (red.), *Trzy wymiary współczesnego bezpieczeństwa*, Warszawa 2014.
Szczygieł M., *Polityka cyberbezpieczeństwa Unii Europejskiej – początek drogi do strategicznej autonomii*, „Sprawy Międzynarodowe" 2018, nr 71(2).
Szewczyk B.M.J., *Rozszerzenie i legitymacja Unii Europejskiej*, „Polski Rocznik Prawa Międzynarodowego" 2010, nr 30.
Szmyd J., *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna*, w: P. Tyrała P. (red.), *Zarządzanie bezpieczeństwem. Międzynarodowa Konferencja Naukowa Kraków 11–13 maja 2000*, Kraków 2000, s. 48.
Szwarc-Kuczer M., *Harmonizacja znamion przestępstw i kar w Traktacie z Lizbony*, „Europejski Przegląd Sądowy" 2009, nr 4.
Szyjko C.T., *Polska w Unii Europejskiej: problemy wyzwania, nadzieje: wybrane aspekty prawne, międzynarodowe i społeczno-gospodarcze*, Warszawa 2014.
Świeboda H., *Infrastruktura informacyjna państwa*, w: P. Kwećka (red.), *Podstawy bezpieczeństwa informacyjnego państwa*, Warszawa 2014.
Świecki D. (red.), *Kodeks postępowania karnego. Komentarz*, t. II, Warszawa 2018.
Tabor M., *Polityka zagraniczna a tożsamość narodowa*, w: J. Kukułka, R. Zięba (red.), *Polityka zagraniczna państwa*, Warszawa 1992.
Tarnogórski R., *Konwencja o cyberprzestępczości – międzynarodowa odpowiedź na przestępczość ery informacyjnej*, w: M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa Polski*, Warszawa 2009.
Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji. Wymagania PN-ISO/IEC

27001, Warszawa 2007.
Timmers P., *The European Union's cybersecurity industrial policy*, „Journal of Cyber Policy" 2018, vol. 3(3).
Tomaszyk M. (red.), *Polityczno-społeczne i ekonomiczne zmiany w świetle globalnej strategii na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej*, Poznań 2017.
Urbanek A., *Współczesny człowiek w przestrzeni bezpieczeństwa*, Słupsk 2015.
Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.
Wawrzusiszyn A., *Bezpieczeństwo, strategia, system. Teoria i praktyka w zarysie,* Warszawa 2015.
Wawrzyk P., *Bezpieczeństwo wewnętrzne Unii Europejskiej*, Warszawa 2009.
Wąsek A., Zawłocki R. (red.), *Kodeks karny. Część szczególna*, t. II: *Komentarz do artykułów 222–316*, Warszawa 2010.
Wąsek A., Zawłocki R. (red.), *Komentarz do Kodeksu karnego. Część szczególna*, Warszawa 2010.
Welsch W., *Sztuczne raje? Rozważania o świecie mediów elektronicznych i innych światach*, w: A. Zeidler-Janiszewska (red.), *Problemy ponowoczesnej pluralizacji kultury. Wokół koncepcji Wolfganga Welscha*, cz. 1, Poznań 1998.
Wessels W., *The Maastricht Treaty and the European Council. The History of an Institutional Evolution*, „Journal of European Integration" 2012, vol. 34(7).
Węc J., *Ewolucja wymiaru sprawiedliwości i spraw wewnętrznych Unii Europejskiej w latach 1992–2001*, „Zeszyt Naukowy" 2010, nr 4.
Wilk A.M., *Państwo w dobie społeczeństwa informacyjnego – perspektywa strategicznych zmian*, w: R. Skubisz (red.), *Internet 2000. Prawo – ekonomia – kultura*, Lublin 2000.
Williams P.D., *Badania bezpieczeństwa. Wprowadzenie*, w: P.D. Williams (red.), *Studia bezpieczeństwa*, Kraków 2012.
Wojciechowski S., *Reasons of Contemporary Terrorism. An Analysis of Main Determinants*, w: A. Sroka, F. Castro-Rial Garrone, R. Torres Kumbrian (red.), *Radicalism and Terrorism in the 21st Century*,

Frankfurt am Main–Bern–Bruxelles–New York–Oxford–Warszawa–Wien 2017.
Wojciechowski S., *Three dimensions of modern terrorism in the European Union*, „Rocznik Integracji Europejskiej" 2018, nr 12.
Wojciechowski Ł., Trubalska J. (red.), *Bezpieczeństwo państwa w cyberprzestrzeni*, Lublin 2017.
Wrona J., *Przestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Białystok 2017.
Wrona J., Witkowska M., Cholawo-Sosnowska K. (red.), *Społeczeństwo informacyjne. Istota. Rozwój. Wyzwania*, Warszawa 2006.
Wróblewska-Łysik M., *Europejska Strategia Globalna a możliwości współpracy Unii Europejskiej z NATO po szczycie w Warszawie*, „Biuro Bezpieczeństwa Narodowego" 2016, nr I–IV.
Wróblewski R., *Przedmiot i metoda nauki o bezpieczeństwie narodowym*, w: P. Sienkiewicz, M. Marszałek, H. Świeboda (red.), *Metodologia badań bezpieczeństwa narodowego*, t. II, Warszawa 2012.
Wyligała H., *Kształtowanie i monitorowanie Strategii Bezpieczeństwa Wewnętrznego Unii Europejskiej*, „Rocznik Bezpieczeństwa Międzynarodowego" 2014, vol. 8(1).
Wyrębek H., Szmitkowski P., *Koncepcja interaktywnego systemu ostrzegania i alarmowania ludności o zagrożeniach*, „Bezpieczeństwo i Technika Pożarnicza" 2018, vol. 50(2).
Verton D., *Black ice. Niewidzialna groźba cyberterroryzmu,* Katowice 2004.
von Clausewitz C., *O wojnie*, Lublin 1995.
Vink M., *Limits of European Citizenship: European Integration and Domestic immigration policies*, „Constitutionalism Web-Papers" 2003.
Zacher L.W., *Odrealnienie człowieka i jego świata – Wstępne refleksje i uwagi*, w: A. Kiepas, M. Sułkowska, M. Wołek (red.), *Człowiek a światy wirtualne*, Katowice 2009.
Zacher L.W., *Transformacje i perspektywy społeczeństw informacyjnych*, „Nierówności społeczne a wzrost gospodarczy", Rzeszów 2013, z. 32.

Zając J., *Bezpieczeństwo państwa*, w: K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), *Bezpieczeństwo państwa: wybrane problemy*, Warszawa 2009.
Zaręba A.M., *Integracja europejska jako konsekwencja II wojny światowej*, w: *Druga wojna światowa: wybrane zagadnienia konfliktu międzynarodowego*, Chełm 2015.
Zaleski S., *Administracja rządowa wobec wyzwań bezpieczeństwa państwa*, Bielsko-Biała 2007.
Zawłocki R., *Przestępstwa przeciwko przedsiębiorcom. Komentarz*, Warszawa 2003.
Zgorzały R., *Przestępstwo o charakterze terrorystycznym w polskim prawie karnym*, „Prokuratura i Prawo" 2007, nr 7–8.
Zherestov P., *From visible pasts to an invisible presence: new criminological reality after planetary cyber attack 12/05/17 Wannacry*, „Przegląd Wschodnioeuropejski" 2018, nr 2.
Ziarko J., *Paradygmaty i orientacje badawcze w nauce o bezpieczeństwie*, „Bezpieczeństwo. Teoria i Praktyka" 2008, nr 1–2.
Zięba A. (red.), *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Warszawa 2008.
Zięba R., *Bezpieczeństwo w ujęciu różnych paradygmatów naukowych*, w: R. Skarzyński, E. Kużelewska (red.), *Bezpieczeństwo. Dyscyplina nauki wobec funkcjonowania państwa*, Białystok 2018.
Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego: koncepcje – struktury – funkcjonowanie*, Warszawa 2004.
Zięba R., *Pojęcie i istota bezpieczeństwa politycznego w stosunkach międzynarodowych,* „Sprawy Międzynarodowe" 1989, nr 1.
Zięba R., *Unia Europejska jako aktor stosunków międzynarodowych*, Warszawa 2003.
Zięba R., *Uwarunkowania polityki zagranicznej państwa*, w: R. Zięba (red.), *Wstęp do teorii polityki zagranicznej państwa*, Toruń 2005.
Zięba R., *Wspólna polityka zagraniczna i bezpieczeństwa Unii Europejskiej*, Warszawa 2007.
Zięba S., *Perspektywy ekologii człowieka*, Lublin 2008.
Ziętek A.W., *Bezpieczeństwo kulturowe w Europie*, Lublin 2013.
Ziller J., *Le traité de Prüm Une vraie-fausse coopération renforcée dans l'Espace de sécurité de liberté et de justice*, „European University

Institute Working Papers LAW" 2006.
Zoll A. (red.), *Kodeks karny. Część szczególna. Komentarz*, Warszawa 2012.
Zyblikiewicz L.W., *Stosunki międzynarodowe jako dyscyplina naukowa*, w: E. Cziomer, L.W. Zyblikiewicz, *Zarys współczesnych stosunków międzynarodowych*, Warszawa 2016.
Żarkowski P. (red.), *Współczesne bezpieczeństwo jednostkowe*, Warszawa–Siedlce 2013.
Żebrowski A., *Walka informacyjna na służbie terrorystów*, cz. 1, „e-Terroryzm.pl" 2014, nr 2.
Żmigrodzki P., *Słownik synonimów i antonimów*, Wrocław 2007.
Żukrowska K., *Globalizacja jako determinanta nowego systemu bezpieczeństwa międzynarodowego*, w: J. Osiński J. (red.), *Globalna gospodarka – lokalne społeczeństwa. Świat u progu XXI wieku*, Warszawa 2001.

Netografia

Challenges to effective EU cybersecurity policy 2019, https://www.eca.europa.eu/ (dostęp: 30.07.2020).
Denning D., *Is Cyber Terror Next?,*www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc (dostęp: 15.07.2020).
Ebbinghaus U., T. Thiel, S. Schulz, *Europäische Datenschutz-reform Machtprobe mit Silicon Valley*, „Frankfurter Allgemeine Zeitung", http://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/europas-it-projekt/digitale-agenda-machtprobe-mit-silicon-valley-12842407.html (dostęp: 11.03.2014).
Fontanella-Khan J., *Victory for tech giants on EU data laws*, „Financial Times", http://www.ft.com/cms/s/5ad18e46-3d8c-11e3-9928-00144feab7de,Authorised=false.html?_i_location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2F5ad18e46-3d8c-11e3-9928-00144feab7de.html%3Fsiteedition%3Duk&siteedition=uk&_i_referer (dostęp: 25.10.2013).
Hollis D., *Cyberwar Case Study: Georgia 2008*, „Small Wars Journal" 2011, http://smallwarsjournal.com/blog/journal/docs-temp/639-

hollis.pdf (dostęp: 12.04.2020).
Jak chińskie Politbiuro wojowało z Google, http://www.tvn24.pl/wiadomosci-ze-swiata,2/jak-chinskie-politbiuro-wojowalo-z-google,154681.html (dostęp: 15.07.2017).
Koziej S., *Braki Strategii Bezpieczeństwa Narodowego 2020: bez koncepcji operacyjnej i priorytetów operacyjnych*, https://pulaski.pl/pulaski-policy-paper-s-koziej-braki-strategii-bezpieczenstwa-narodowego-2020-bez-koncepcji-operacyjnej-i-priorytetow-preparacyjnych/ (dostęp: 20.07.2020).
Lynn W.J., Thompson N., *The Pentagon's New Cyberstrategy*, Foreign Affairs, October 1, 2010, https://www.foreignaffairs.com/articles/2011-09-28/pentagons-cyberstrategy-one-year-later (dostęp: 14.07.2020).
Łapczyński M., *Zagrożenia cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*, https://pulaski.pl/wp-content/uploads/2015/02/Pulaski_Policy_Papers_No_7_09.pdf (dostęp: 14.07.2020).
Maj P., *Cyberterroryzm w stosunkach międzynarodowych*, http://www.politologia.pl/fck_pliki/File/consensus/consensus_1.pdf (dostęp: 15.12.2017).
Nowak L., *O ukrytej jedności nauk społecznych i nauk przyrodniczych*, http://www.staff.amu.edu.pl/~epistemo/Nowak/przyrhum.pdf (dostęp: 21.10.2009).
Podręcznik europejskiego prawa o ochronie danych, Agencja Praw Podstawowych Unii Europejskiej 2014, Rada Europy 2014, Luksemburg: Urząd Publikacji Unii Europejskiej 2014 r., s. 16 dostępne: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ae65e (dostęp: 27.07.2020).
Warman M., *EU Privacy regulations subject to unprecedented lobbying*, „The Telegraph"; http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html (dostęp: 02.08.2012).
cirbw.de umziehen (dostęp: 07.07.2020).

„e-Terroryzm.pl” 2013, nr 5(17).
http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/livre_blanc_tome1_partie1.pdf (dostęp: 30.07.2020).
http://bip.msw.gov.pl/bip/programy/19057, dok.html (dostęp: 2.07.2020).
http://eur-lex.europa.eu/legal-content/en/ALL/?uri=OJ:C:2010:083:TOC (dostęp: 16.07.2020).
http://eurlex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24221 (dostęp:10.08.2020).
http://europa.eu/rapid/press-release_IP-96-688_en.htm?locale=en (dostęp:10.08.2020).
http://europa.eu/rapid/press-release_MEMO-17-3194_en.pdf (dostęp: 19.04.2018).
http://lobbyplag.eu/governments/, Schütz, Karaboga 2015, s. 10.
http://www.antyterroryzm.gov.pl/CAT/antyterroryzm/wspolpraca-zagraniczna/walka-z finansowaniem/565,Walka-z-finansowaniem-terroryzmu.html (dostęp: 30.06.2020).
http://www.bmvg.de/ *(*dostęp: 07.07.2017).
http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html (dostęp: 15.07.2020).
http://www.consilium.europa.eu/pl/policies/cyber-security/ (dostęp: 13.08.2018).
http://www.cvce.eu/content/publication/1997/10/13/b0633a76-4cd7-497f-9da14db3dbbb56e8/publishable_en.pdf [20.02.2016]. 92. (dostęp: 14.07.2020).
http://www.cyberdefence24.pl/625839,niemiecka-agencja-cyberbezpieczenstwa-powazne-skutki-ataku-hakerow (dostęp: 7.07.2020).
http://www.export.gov/safeharbor (dostęp: 20.07.2020).
http://www.kooperationssysteme.de/2013/04/05/forschungszentrum-cyber-operations-defence-code/lang-pref/de/ (dostęp: 11.07.2017).
http://www.msz.gov.pl (dostęp: 30.06.2020).
http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (dostęp:

6.07.2020).
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf (dostęp: 30.07.2020).
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf (dostęp: 30.07.2020).
https://ec.europa.eu/digital-single-market/en/cyber-security.
https://ec.europa.eu/poland/news/170919_cyber_attacks_pl.
https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF.
https://eeas.europa.eu/top_stories/pdf/eugs_pl_.pdf. (dostęp: 13.08.2020).
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0477:FIN.
https://securelist.com/it-threat-evolution-q1-2020-statistics/96959/.
https://webarchive.nationalarchives.gov.uk/20121018134855/http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf (dostęp: 30.07.2020).
https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf (dostęp: 30.06.2020).
https://www.bbn.gov.pl/ftp/SBN%20RP.pdf (dostęp: 30.06.2020).
https://www.bsi.bund.de (dostęp: 11.07.2017).
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5 (dostęp: 11.07.2017).
https://www.bundeswehr.de (dostęp: 11.07.2017).
https://www.consilium.europa.eu/.
https://www.consilium.europa.eu/media/37024/st14413-en18.pdf.
https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html (dostęp 30.07.2020).
https://www.enisa.europa.eu/news/enisanews/standard-operational-procedures-to-manage-multinational-cyber crises-finalised-by-eu-efta-memberstates-and-enis (dostęp: 15.05.2020).

https://www.gov.uk/government/publications/cyber-security-strategy (dostęp: 30.07.2020).
https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021(dostęp: 30.07.2020).
https://www.irsem.fr/data/files/irsem/documents/document/file/105/20170707-NP-CICDE-DIA-3.0.3-ASI-2017.pdf (dostęp: 30.07.2020).
https://www.itu.int/dms_pub/itu-d/opb/strategy/D-STR-GCI.01-2017-PDF-E.pdf (dostęp: 10.08.2020).
https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf (dostęp: 30.07.2020).
https://www.ons.gov.uk/ (dostęp: 15.08.2020).
https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/ (dostęp: 30.07.2020).
https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-0215_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf (dostęp: 30.07.2020).
https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf (dostęp: 10.08.2020).
www.coe.int/gmt (dostęp: 30.04.2012).
www.coe.int/terrorism (dostęp: 30.04.2012).
www.defense.gouv.fr/content/download/237708/2704474/file/Pacte%20D%C3%A9fense%Cyber-1.pdf (dostęp: 30.07.2020).
www.legifrance.gouv.fr/affichTexte.do?cid-Texte=JORFTEXT000030931899&categorieLien=id (dostęp: 30.07.2020).

O AUTORCE

dr hab. Izabela Oleksiewicz jest profesorem Politechniki Rzeszowskiej im. Ignacego Łukasiewicza. Jej zainteresowania badawcze to polityka antycyberterrorystyczna UE, polityka antyterrorystyczna UE, polityka uchodzcza UE oraz bezpieczenstwo w obszarze transaltantyckim.

PRZYPISY

[1] Por. E. Milczarek, *Współczesne wyzwania ochrony bezpieczeństwa informacyjnego jednostki w Internecie*, w: M. Porzeżyński, A. Borcuch (red.), *Bezpieczeństwo w erze społeczeństwa informacyjnego. Wyzwania w sferach kultury, marketingu i gospodarki,* Kielce 2019, s. 85–87.

[2] J. Szmyd, *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna*, w: P. Tyrała (red.), *Zarządzanie bezpieczeństwem*. Międzynarodowa Konferencja Naukowa Kraków 11–13 maja 2000, Kraków 2000, s. 48.

[3] H. Batorowska, P. Motylińska, *Bezpieczeństwo informacyjne i medialne w czasach nadprodukcji informacji,* Warszawa 2020, s. 98.

[4] Por.: A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 298–300. A. Becla, *Społeczeństwo informacyjne i społeczeństwo pseudoinformacyjne – problemy pojęciowe i metodyczne identyfikacji*, „Handel Wewnętrzny" 2012, t. 3.

[5] Szerzej: R. Siudak, *5G Szanse – zagrożenia – wyzwania*, Kraków 2020, s. 5–7.

[6] Por.: J. Gryz, *Wzajemny związek między polityką i strategią a bezpieczeństwem państwa*, „Rocznik Bezpieczeństwa Międzynarodowego" 2007, nr 2, s. 15.

[7] A. Adamski, *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005, nr 4 (167).

[8] Por.: Raport roczny za 2019 r.; z http://kaspersky.pl za 2019 r. (dostęp: 13.08.2020).

[9] J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996, s. 18.

[10] K. Kasowska-Pedrycz, *Polityka bezpieczeństwa wewnętrznego UE – ewolucja i perspektywy*, w: R. Bäcker, J. Marszałek-Kawa, J. Modrzyńska (red.), *Od starej do nowej Europy?*, Toruń 2005, s. 87.

[11] W. Fehler, *O pojęciu bezpieczeństwa informacyjnego*, w: M. Kubiak, S. Topolewski (red.), *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce–Warszawa 2006, s 37.

[12] K. Prokop, *Ocena norm konstytucyjnych dla realizacji skutecznego systemu bezpieczeństwa narodowego, ze szczególnym uwzględnieniem stanu wojny. Ocena stanu obecnego i rekomendacje na przyszłość*, materiał opracowany na potrzeby SPBN, BBN, Warszawa 2011.

[13] I. Oleksiewicz, M. Polinceusz, M. Pomykała (red.), *Nowoczesne technologie – źródło zagrożeń i narzędzie ochrony bezpieczeństwa*, Rzeszów 2014.

[14] W. Krztoń, *Walka o informację w cyberprzestrzeni w XXI wieku*, Warszawa 2017, s. 140–142.
[15] W. Gibson, *Neuromancer*, Warszawa 2001, s. 69.
[16] P. Lévy, *Drugi potop*, w: M. Hopfinger (red.), *Nowe media w komunikacji społecznej w XX wieku*, Warszawa 2002, s. 380.
[17] M. Golka, *Bariery w komunikowaniu i społeczeństwo dezinformacyjne*, Warszawa 2008, s. 99.
[18] A. Charyton, *Wpływ Internetu na funkcjonowanie nastolatków*, w: R. Skubisz (red.), *Internet 2000. Prawo – ekonomia – kultura*, Lublin 2000, s. 387.
[19] M. Castells, *Społeczeństwo sieci*, Warszawa 2010, s. 378.
[20] W. Welsch, *Sztuczne raje? Rozważania o świecie mediów elektronicznych i innych światach*, w: A. Zeidler-Janiszewska (red.), *Problemy ponowoczesnej pluralizacji kultury. Wokół koncepcji Wolfganga Welscha*, cz. 1, Poznań 1998, s. 176.
[21] Por.: H. Braun, *The non-military threat spectrum*, „SIPRI Yearbook", London 2003, s. 279.
[22] S. Lem, *Bomba megabitowa*, Kraków 1999, s. 48.
[23] W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych*, wyd. 18, Warszawa 1989, s. 548.
[24] K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 1, s. 16–17.
[25] M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, „Przegląd Teleinformatyczny" 2018, nr 12, s. 60 i n.
[26] W. Krztoń, *Walka o informację*, s. 89–91.
[27] I. Oleksiewicz, *Zarys polityki cyberbezpieczeństwa Unii Europejskiej. Casus Polski i RFN*, Warszawa 2019, s. 32.
[28] D. Brzeziński, *Wolność i bezpieczeństwo w płynnej nowoczesności*, „Studia Socjologiczno-Polityczne" 2017, vol. 6 (1), s. 67.
[29] J. Wrona, M. Witkowska, K. Cholawo-Sosnowska (red.), *Społeczeństwo informacyjne. Istota. Rozwój. Wyzwania*, Warszawa 2006, s. 13.
[30] Y. Masuda, *The Information Society as Post-Indrustial Society*, Washington 1983; J.S. Nowak, G. Bliźniuk (red.), *Społeczeństwo informacyjne: doświadczenie i przyszłość*, Katowice 2006, s. 9.
[31] Termin ten oznacza społeczeństwo komunikujące się przez komputer.
[32] Szerzej: *Report on Europe and the global information society. Interim report on trans-European networks Progress report on employment Extracts of the conclusions of the Presidency of the Corfu European, Council*, „Bulletin of EU", Supplement 2/94, s. 13.
[33] Europe and the Global Information Society: Recommendations to the European Council, Brussels, 26 May 1994.
[34] COM(93) 0700 final.
[35] COM(96) 389 final, 24.06.1996.
[36] Dokument dostępny na oficjalnej stronie internetowej KE w języku angielskim: http://europa.eu/rapid/press-release_IP-96-688_en.htm?locale=en

(dostęp: 10.08.2020).

[37] Jako priorytet UE przyjęła umożliwienie powszechnego dostępu do Internetu. Plan mający na celu budowę europejskiego społeczeństwa informacyjnego został opracowany 23–24 marca 2000 r. w Lizbonie na specjalnym posiedzeniu RE. Zyskał nazwę Strategii lizbońskiej. Plan działania został opracowany na dwóch płaszczyznach: gospodarczej i społecznej. Płaszczyzna gospodarcza budowy społeczeństwa informacyjnego miała się opierać na wykorzystaniu ICT w celu zwiększenia konkurencyjności gospodarki. Z kolei sfera społeczna opierała się na koncepcji Luca Soete'a, który uznał społeczeństwo informacyjne za „społeczeństwo, które właśnie się kształtuje, w którym technologie gromadzenia oraz transformacji informacji i danych są powszechnie dostępne po niskich kosztach".

[38] COM(2002) 263 final, 28.05.2002.

[39] Por.: J. Wrona, *Przestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Białystok 2017, s. 23.

[40] S. Buregwa-Czuma, K. Garwol, *Definicje, właściwości i funkcje społeczeństwa informacyjnego*, s. 30–32.

[41] J.S. Nowak, G. Bliźniuk (red.), *Społeczeństwo informacyjne*, s. 10.

[42] P. Sienkiewicz, *Teoria rozwoju społeczeństwa informacyjnego*, Kraków 2004, s. 506–507.

[43] J. Pawłowski (red.), *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2002, s. 78.

[44] Urządzenia elektroniczne wchodzące w skład infrastruktury teleinformatycznej niezbędnej do należytego gromadzenia, przetwarzania, przechowywania i wymiany informacji. Infrastrukturę tę tworzą przede wszystkim sieć Internet i inne sieci teleinformatyczne. P. Dela, *Teoria walki w cyberprzestrzeni*, Warszawa 2020.

[45] P. Dela, *Zasady sztuki wojennej w cyberprzestrzeni*, w: A. Polak, J. Lasota, M. Palczewska (red.), *Wojny i konflikty zbrojne XXI wieku – podejście polemologiczne*, Warszawa 2016, s. 314.

[46] S. Jaskuła, *Informacyjna przestrzeń tożsamości*, Warszawa 2010, s. 1.

[47] R. Kwećka, *Strategia bezpieczeństwa informacyjnego państwa*, Warszawa 2014, s. 25.

[48] P. Timmers, *The European Union's cybersecurity industrial policy*, „Journal of Cyber Policy" 2018, vol. 3(3), s. 363–366.

[49] H. Świeboda, *Infrastruktura informacyjna państwa*, w: R. Kwećka (red.), *Podstawy bezpieczeństwa informacyjnego państwa*, Warszawa 2014, s. 57.

[50] J. Oleński, *Ekonomika informacji. Metody*, Warszawa 2003, s. 15.

[51] S. Zaleski, *Administracja rządowa wobec wyzwań bezpieczeństwa państwa*, Bielsko-Biała 2007, s. 96.

[52] R. Kwećka, *Zarys teorii bezpieczeństwa informacyjnego państwa*, w: J. Gryz (red.), *Zarys teorii bezpieczeństwa państwa*, Warszawa 2016, s. 162.

[53] W. Steinmüller, *Zautomatyzowane systemy informacyjne w administracji prywatnej i publicznej*, „Organizacja – Metoda – Technika" 1977, nr 9, s. 21.
[54] Wspólne źródłosłowie angielskich i polskich wyrażeń: *communication* – komunikowanie, *community* – społeczność od łacińskiego *communicatio* – wymiana, łączność, *communis* – współdziałanie, współodpowiedzialność oraz *communitas* – wspólnota, wspólnotowość.
[55] Zob.: J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013, s. 13.
[56] S. Jarmoszko, *Bezpieczeństwo kulturowe i kultura bezpieczeństwa jako kategorie antropologiczne*, w: P. Żarkowski, S. Tobolewski (red.), *Współczesne bezpieczeństwo kulturowe*, Siedlce 2014, s. 159. Zob. też: A.W. Ziętek, *Bezpieczeństwo kulturowe w Europie*, Lublin 2013, s. 78.
[57] Zob.: A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2007, s. 361.
[58] Zob.: J. Oleński, *Ekonomika informacji*, s. 164.
[59] Zob.: J. Łuczak (red.), *Zarządzanie bezpieczeństwem informacji*, Poznań 2004, s. 63.
[60] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006, s. 7.
[61] Zob.: W. Pokruszyński, *Bezpieczeństwo: teoria i praktyka*, Józefów 2012, s. 42.
[62] P. Bączek, *Zagrożenia informacyjne*, s. 56.
[63] Por: P. Żarkowski (red.), *Współczesne bezpieczeństwo jednostkowe*, Warszawa–Siedlce 2013, s. 289–299.
[64] Zob.: *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji. Wymagania PN-ISO/IEC 27001*, Warszawa 2007, s. 9; J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne*, s. 19–20.
[65] A. Drozd, *Ustawa o ochronie danych*, s. 361.
[66] Por.: W. Krztoń, *Walka o informację*, s. 82–85.
[67] M. Chapple, D. Seidl, *Cyberwarfare: Information Operations in a Connected World*, Burlington 2015, s. 172.
[68] M. Górka, *Istota bezpieczeństwa cybernetycznego w polityce państw Grupy Wyszehradzkiej w latach 2013–2017*, Toruń 2019, s. 235.
[69] W. Wessels, *The Maastricht Treaty and the European Council. The History of an Institutional Evolution*, „Journal of European Integration" 2012, vol. 34(7), s. 755–756.
[70] Szerzej: rozdział 4.2.
[71] Rozporządzenie Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (*Dz.Urz. UE UE L 129 z 17.05.2019)*.
[72] Oświadczenie Daniela Castro, wiceprezesa ITIF, zamieszczone m.in. na łamach „Dziennika Internautów Biznes i Prawo" 7.10.2015. Por.: http://di.com.pl/opinie-wyrok-ws-safe-harbour-niczym-przecinanie-podmorskich-kabli-co-na-to-polski-giodo-53374 (dostęp: 15.11.2020).

[73] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Paris 1980; http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (dostęp: 6.07.2020).

[74] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Reference, CETS No. 108 (1981); http://www.coe.int/pl/web/conventions/full-list/-/conventions/treaty/108 (dostęp: 06.07.2020).

[75] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Brussels 1995; http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046 (dostęp: 20.07.2020).

[76] Więcej na temat programu *Safe Harbor* zob.: http://www.export.gov/safeharbor (dostęp: 20.07.2020).

[77] 6 października 2015 r. Trybunał Sprawiedliwości UE wydał ostateczne orzeczenie o nieważności decyzji KE z dnia 26 lipca 2000 r. stwierdzającej, że USA zapewniają odpowiedni poziom ochrony danych osobowych zgodny ze standardami UE. Trybunał rozpoznawał sprawę C-362/14 zainicjowaną przez austriackiego aktywistę Maxa Schremsa, prywatnego użytkownika serwisu Facebook, który po doniesieniach Edwarda Snowdena, że Stany Zjednoczone nie zapewniają danym obywateli UE przesyłanym do USA żadnej rzeczywistej ochrony przed nadużyciami ze strony amerykańskich władz, wystąpił do irlandzkiego organu ochrony danych ze skargą na naruszenie jego praw do ochrony danych. Organ irlandzki oddalił ją, powołując się na decyzję KE o *Safe Harbor*. Schrems nie dał jednak za wygraną i odwołał się do irlandzkiego Sądu Najwyższego, który następnie skierował do Trybunału Sprawiedliwości UE zapytanie, czy wobec przedmiotowej decyzji KE krajowy organ nadzoru jest uprawniony do rozpoznania skargi Schremsa, przeprowadzenia postępowania w sprawie nieodpowiedniego poziomu ochrony danych skarżącego oraz – w razie stwierdzenia naruszenia ustawodawstwa UE – do zarządzenia zaprzestania przekazywania danych obywateli UE do USA. Rozpoznawszy sprawę, Trybunał UE orzekł, że decyzja KE nie ogranicza uprawnień, jakie przysługują krajowym organom nadzorczym, i w związku z tym organy te są zobowiązane do rozpoznawania odnośnych skarg obywateli UE i wydawania orzeczeń w sprawach, czy przekazywanie do USA danych osobowych podlegających ochronie na terytorium UE spełnia wymogi prawodawstwa UE. Trybunał orzekł ponadto, że jakiekolwiek uregulowania pozbawiające obywatela UE możliwości podjęcia kroków prawnych w celu uzyskania dostępu do dotyczących go danych osobowych naruszają obowiązujące w UE podstawowe prawo obywatela do skutecznej ochrony sądowej. Jednocześnie podzielił wątpliwości skarżącego, że USA nie mogą być bezwzględnie uznawane za „bezpieczną przystań” dla

podlegających ochronie danych osobowych obywateli UE, i uznał decyzję KE w tej sprawie za nieważną.

[78] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML (dostęp: 16.07.2020).

[79] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services; Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws; http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009L0136 (dostęp: 16.07.2020).

[80] Karta praw podstawowych Unii Europejskiej (Amtsblatt C 83 (2010), s. 389–403); http://eur-lex.europa.eu/legal-content/en/ALL/?uri=OJ:C:2010:083:TOC (dostęp: 16.07.2020).

[81] Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (COM(2012) 0011 final), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:PL:PDF (dostęp: 16.07.2020).

[82] Dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych (COM(2012) 0010 final), http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52012PC0010&from=EN (dostęp: 16.07.2020).

[83] Por.: M. Warman, *EU Privacy regulations subject to unprecedented lobbying*, „The Telegraph"; http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html (dostęp: 02.08.2012).

[84] Wyrok SA Kraków z 19.12.2000 r., I Aca 794/00, TPP 2002, nr 3, s. 137.

[85] Szerzej: K. Michalski, I. Oleksiewicz, K. Sienkiewicz, *Bezpieczeństwo online i offline*, Warszawa 2017, s. 33–38.

[86] P. Schütz, *Zum Leben zu wenig, zum Sterben zu viel? Die finanzielle und personelle Ausstattung deutscher Datenschutzbehörden im Vergleich*, w: A. Roßnagel i wsp. (red.), *Die Zukunft des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung*, Wiesbaden 2018, s. 251.

[87] Odpowiednia dokumentacja znajduje się na platformie demaskatorskiej lobbyplag.eu; http://lobbyplag.eu/lp.

[88] Por.: J. Fontanella-Khan, *Victory for tech giants on EU data laws*, „Financial Times", http://www.ft.com/cms/s/5ad18e46-3d8c-11e3-9928-00144feab7de,Authorised=false.html?_i_location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2F5ad18e46-3d8c-11e3-9928-00144feab7de.html%3Fsiteedition%3Duk&siteedition=uk&_i_referer (dostęp: 25.10.2013); U. Ebbinghaus, T. Thiel, S. Schulz, *Europäische Datenschutz-reform Machtprobe mit Silicon Valley*, „Frankfurter Allgemeine Zeitung", http://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/europas-it-projekt/digitale-agenda-machtprobe-mit-silicon-valley-12842407.html (dostęp: 11.03.2014).

[89] Por.: http://lobbyplag.eu/governments/, Schütz, Karaboga 2015, s. 10.

[90] *Policy paper. Foreign policy, defence and development – a future partnership*, paper https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643924/Foreign_policy__defence_and_development_paper.pdf (dostęp: 30.07.2020).

[91] *Powszechna encyklopedia filozofii*, Lublin 2007.

[92] *Encyklopedia PWN*, Warszawa 2010, t. 12, s. 86.

[93] Por.: W. Kopaliński, *Słownik wyrazów*, s. 512.

[94] T.S. Kuhn, *Struktura rewolucji naukowych*, Warszawa 2001, s. 10.

[95] T. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016, s. 167.

[96] I. Lakatos, A. Musgrave (red.), *Criticism and the Growth of Knowledge*, Cambridge 1999, s. 199.

[97] Szerzej: L. Nowak, *O ukrytej jedności nauk społecznych i nauk przyrodniczych*, http://www.staff.amu.edu.pl/~epistemo/Nowak/przyrhum.pdf (dostęp: 21.10.2009).

[98] T.S. Kuhn, *Raz jeszcze o paradygmatach*, w: *Dwa bieguny. Tradycja i nowatorstwo w badaniach naukowych*, T.S. Kuhn, Warszawa 1985, s. 320–325.

[99] Por.: A. Matysiak, M. Struś, *Paradygmat rozwoju zrównoważonego,* „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2015, nr 213, s. 13–14.

[100] Ibidem, s 14.

[101] J. Kukułka, *Bezpieczeństwo, a współpraca europejska: współzależności i sprzeczności interesów*, „Sprawy Międzynarodowe" 1982, nr 7, s. 31.

[102] J. Stańczyk, *Współczesne pojmowanie*, s. 17–18.

[103] Zob.: A. Urbanek, *Współczesny człowiek w przestrzeni bezpieczeństwa*, Słupsk 2015, s. 188.

[104] Zob. M. Cieślarczyk, *Kultura bezpieczeństwa i obronności*, Siedlce 2006, s. 23.

[105] R. Zięba, *Bezpieczeństwo w ujęciu różnych paradygmatów naukowych*, w: R. Skarzyński, E. Kużelewska, *Bezpieczeństwo. Dyscyplina nauki wobec funkcjonowania państwa*, Białystok 2018, s. 14–16.

[106] J. Czaputowicz, *System czy nieład? Bezpieczeństwo europejskie u progu XXI wieku*, Warszawa 1998, s. 52.
[107] Por.: A. Niedźwiecki, *Paradygmat liberalny wobec problemu dezintegracji instytucji międzynarodowych*, „Przegląd Zachodni" 2019, nr 2, s. 8–9.
[108] A. Moravcsik, *Liberal International Relations Theory: A Scientific Assessment*, w: C. Elman, M. Fendius Elman (red.), *Progress in International Relations Theory: Appraising the Field*, Cambridge 2003, s. 2.
[109] A. Moravcsik, *Taking Preferences Seriously: A Liberal Theory of International Politics*, „International Organization" 2007, nr 4(51), s. 514.
[110] Por.: M. Avbelj, *Brexit: An End to the End of History*, „German Law Journal" 2016, vol. 17, s. 2.
[111] P.D. Williams, *Badania bezpieczeństwa. Wprowadzenie*, w: P.D. Williams (red.), *Studia bezpieczeństwa*, Kraków 2012, s. 87–98.
[112] J. Ziarko, *Paradygmaty i orientacje badawcze w nauce o bezpieczeństwie*, „Bezpieczeństwo. Teoria i Praktyka" 2008, nr 1–2, s. 9–22.
[113] Por.: B. Hołyst, *Bezpieczeństwo. Ogólne problemy badawcz*e, Warszawa 2014, s. 170.
[114] S. Jarmoszko, *Antropologia bezpieczeństwa. Kontury naukowej tożsamości*, Siedlce 2015, s. 35–38.
[115] S. Sulowski, *Państwo i bezpieczeństwo w kazualnym związku*, w: S. Sulowski, M. Brzeziński (red.), *Trzy wymiary współczesnego bezpieczeństwa*, Warszawa 2014, s. 14.
[116] Por.: A. Pieczywok, K. Loranty (red.), *Bezpieczeństwo jako problem edukacyjny*, Warszawa 2015, s. 148–152.
[117] A. Piątek, *Edukacja na rzecz bezpieczeństwa*, Warszawa 2011, s. 10.
[118] Por.: R. Wróblewski, *Przedmiot i metoda nauki o bezpieczeństwie narodowym*, w: P. Sienkiewicz, M. Marszałek, H. Świeboda (red.), *Metodologia badań bezpieczeństwa narodowego*, t. II, Warszawa 2012, s. 31–46.
[119] T.R. Aleksandrowicz, K. Liedel, *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia*, w: K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo*. *Wojna, pokój i terroryzm w epoce informacji*, Warszawa 2014, s. 22–24.
[120] K. Raczkowski, K. Żukrowska, M. Żuber (red.), *Interdyscyplinarność nauk o bezpieczeństwie. Paradygmat*. *Wiedza*. *Demarkacja*, Warszawa 2013, s. 124.
[121] Por.: D. Kowalski, M. Kwiatkowski, A. Zduniak (red.), *Edukacja dla bezpieczeństwa – wybrane perspektywy*, Lublin–Poznań 2004, s. 134.
[122] S. Zięba, *Perspektywy ekologii człowieka*, Lublin 2008, s. 171–173.
[123] Zob.: T. Jemioło, A. Dawidczyk, *Wprowadzenie do metodologii badań bezpieczeństwa*, Warszawa 2008, s. 43–84.
[124] P. Sienkiewicz, *Natura bezpieczeństwa w perspektywie systemowe*j, w: K. Drabik (red.), *Natura bezpieczeństwa w perspektywie personalnej i strukturalnej*, Warszawa 2013, s. 56–57.
[125] B. Hołyst, *Bezpieczeństwo społeczeństwa*, Warszawa 2015.

[126] W. Gizicki, *Polityczne uwarunkowania bezpieczeństwa europejskiego*, Toruń 2008, s. 34–40.
[127] J. Gryz, *Paradygmaty bezpieczeństwa*, w: P. Sienkiewicz, M. Marszałek, H. Świeboda (red.), *Metodologia badań bezpieczeństwa narodowego*, t. II, Warszawa 2011, s. 132.
[128] J. Kunikowski, *Wiedza i edukacja dla bezpieczeństwa*, Warszawa 2002, s. 90.
[129] G.J. Rattray, *Wojna strategiczna w cyberprzestrzeni*, Warszawa, 2000, s. 34.
[130] W. Pokruszyński, *Polityka a strategia bezpieczeństwa*, Józefów 2011, s. 43 i n.
[131] A. Wawrzusiszyn, *Bezpieczeństwo, strategia, system. Teoria i praktyka w zarysie*, Warszawa 2015, s. 25.
[132] M. Łapczyński, *Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*, „Pułaski Policy Papers" 2009, nr 7, s. 5.
[133] C. von Clausewitz, *O wojnie*, Lublin 1995, s. 23.
[134] Ibidem, s. 25.
[135] B.H. Liddell Hart, *Strategia działań pośrednich*, Warszawa 1959, s. 388.
[136] A. Beaufre, *Wstęp do strategii. Odstraszanie i strategia*, Warszawa 1968, s. 46–47.
[137] Ibidem, s. 30.
[138] T. Aleksandrowicz, *Strategia bezpieczeństwa narodowego Polski*, Warszawa 2013.
[139] A.M. Zaręba, *Integracja europejska jako konsekwencja II wojny światowej*, w: *Druga wojna światowa: wybrane zagadnienia konfliktu międzynarodowego*, Chełm 2015.
[140] F. Skibiński, *Rozważania o sztuce wojennej*, Warszawa 1972, s. 103 i 109.
[141] Szerzej: W. Pokruszyński, *Polityka – Teoria – Bezpieczeństwo*, Józefów 2012, s. 44–45.
[142] A. Zięba (red.), *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Warszawa 2008, s. 56.
[143] P. Soroka, *Polistrategia bezpieczeństwa zewnętrznego Polski. Ujęcie normatywne*, Warszawa 2005, s. 121.
[144] R. Zięba, *Pojęcie i istota bezpieczeństwa politycznego w stosunkach międzynarodowych*, „Sprawy Międzynarodowe" 1989, nr 1, s. 27–29.
[145] M. Ciecierski, *Wywiad biznesowy w korporacjach transnarodowych. Teoria i praktyka,* Toruń 2009, s. 17–21.
[146] C.T. Szyjko, *Polska w Unii Europejskiej: problemy wyzwania, nadzieje: wybrane aspekty prawne, międzynarodowe i społeczno-gospodarcze,* Warszawa 2014, s. 95.
[147] W. Pokruszyński, *Współczesne bezpieczeństwo narodowe*, Józefów 2009, s. 24; Por.: P. Soroka, *Polistrategia bezpieczeństwa zewnętrznego Polski*, Warszawa 2005, s. 136.
[148] Por.: H. Korczyk, *Bezpieczeństwo i rozbrojenie w projektach Ligi Narodów*, „Mazowieckie Studia Humanistyczne" 2005, nr 1–2, s. 43–54.
[149] Główne przesłanie brzmiało: „Koncepcja interesu narodowego […] zakłada nieustający konflikt i groźbę wojny, które winno się pomniejszać przez stałe

przystosowywanie sprzecznych interesów dzięki działaniu dyplomacji". Zob.: L.W. Zyblikiewicz, *Stosunki międzynarodowe jako dyscyplina naukowa*, w: E. Cziomer, L.W. Zyblikiewicz, *Zarys współczesnych stosunków międzynarodowych*, Warszawa 2016, s. 13–23.

[150] Por.: J. Czaja, *Kulturowy wymiar bezpieczeństwa. Aspekty teoretyczne i praktyczne*, Kraków 2013, s. 47.

[151] M. Adamska (red.), *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna,* Warszawa, 2013, s. 46.

[152] W. Pokruszyński, *Uwarunkowania współczesnego bezpieczeństwa międzynarodowego*, Szczytno 2006, s. 66.

[153] J. Baylis, *Bezpieczeństwo międzynarodowe i globalne w epoce pozimnowojennej*, w: *Globalizacja polityki światowej. Wprowadzenie do stosunków międzynarodowych*, Kraków 2008, s. 365–366.

[154] J. Czaputowicz, *Bezpieczeństwo w teoriach stosunków międzynarodowych*, Warszawa 2007, s. 50.

[155] J. Reginia-Zacharski, I. Oleksiewicz, I. Topolski, *The faces of the modern World. Political dimmention*, Berlin 2018, s. 46.

[156] M. Soja, *Stosunki UE–NATO w dziedzinie bezpieczeństwa europejskiego i obrony na przełomie XX i XXI wieku*, Warszawa 2011, s. 45.

[157] Tak twierdzili w 1966 r. socjologowie Peter Berger i Thomas Luckman. Zob.: P. Berger, T. Luckman, *The Social Construction of Reality. A Treatise in the Sociology of Knowledge*, New York 1966, s. 23–31.

[158] Głównymi pojęciami wypracowanymi przez nich stały się „sektory bezpieczeństwa", „regionalne kompleksy bezpieczeństwa" i teoria „sekurytyzacji". Uczeni ci przyczynili się do ugruntowania szerokiego ujęcia bezpieczeństwa, w którym elementy militarne oraz inne siłowe mają relatywnie małe znaczenie.

[159] Swoje poglądy zaprezentowali w publikacji: B. Buzan, O. Wæver, J. de Wilde, *Security: A New Framework for Analysis*, Colorado 1998, s. 21–49.

[160] I. Protasowicki, Z. Nowakowski, *Działania Unii Europejskiej na rzecz bezpieczeństwa informacyjnego*, Warszawa 2013, s. 134.

[161] T.R. Aleksandrowicz, *Sieciowy paradygmat bezpieczeństwa państwa w stosunkach międzynarodowych*, Warszawa 2013, s. 65.

[162] M. Karpiuk, K. Prokop, *Bezpieczeństwo państwa. Zagadnienia prawne i administracyjne*, Olsztyn 2016, s. 45.

[163] J. Czaputowicz, *Kryteria bezpieczeństwa międzynarodowego państwa – aspekty teoretyczne,* w: *Kryteria bezpieczeństwa międzynarodowego państwa*, Warszawa 2003, s. 90.

[164] Za: A.D. Rotfeld, *Bezpieczeństwo międzynarodowe czasu przemian*, Warszawa 2004, s. 5.

[165] S. Parzymies, *Stan debaty na temat federalnego kształtu Unii Europejskiej*, w: J. Zając, A. Włodkowska-Bagan, M. Kaczmarski (red.), *Bezpieczeństwo międzynarodowe. Polska – Europa – Świat*, Warszawa 2015, s. 177.

[166] *Europejska strategia bezpieczeństwa. Bezpieczna Europa w lepszym świecie*, Bruksela, 12 grudnia 2003.

[167] Plan Działań Unii Europejskiej w zakresie zwalczania terroryzmu, przyjęty przez nadzwyczajne posiedzenie Rady Europejskiej w Brukseli 21 września 2001 r.; decyzja ramowa Rady Europejskiej 2002/475/WSiSW z 13 czerwca 2002 r. w sprawie zwalczania terroryzmu; decyzja ramowa w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi. Zob.: *Terroryzm: europejska riposta*, Komisja Europejska, Dyrekcja Generalna ds. Sprawiedliwości, Wolności i Bezpieczeństwa, Bruksela, sierpień 2004 r., http://ec.europa.eu/justice_home/key_issues/terrorism/terrorism_0904_pl.pdf. (dostęp: 8.07.2020).

[168] Por.: R. Kuźniar, *Europejska strategia bezpieczeństwa*, „Polska w Europie" 2004, nr 2(46), s. 23.

[169] Por.: M. Soja, *Samorząd terytorialny w procesie integracji europejskiej. Polskie doświadczenia i wnioski na przyszłość*, Katowice 2008, s. 240–245.

[170] J. Lindley-French, F. Algieri, *A European Defence Strategy*, Güetersloh 2004, s. 9, http://www.cap.uni-muenchen.de/download/2004/2004_Venusberg_Report.pdf. (dostęp: 20.07.2020).

[171] *Report on the Implementation of the European Security Strategy*, S407/08, Brussels, 11 December 2008, *https://www.consilium.europa.eu/uedocs/.../reports/104630.pdf* (dostęp: 13.08.2018).

[172] J. Barcz, E. Kawecka-Wyrzykowska, K. Michałowska-Gorywoda, *Integracja europejska w okresie przemian*, Warszawa 2016, s. 45.

[173] *i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia* (COM(2005) 229, 1.06.2005).

[174] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010, s. 36–37.

[175] Szerzej: I. Oleksiewicz, K. Stachurska-Szczesiak, *Oszustwo komputerowe a polityka bezpieczeństwa informacyjnego Polski*, w: P. Bogdalski i in. (red.), *Współczesne zagrożenia cyberterrorystyczne i bioterrorystyczne a bezpieczeństwo narodowe Polski*, Warszawa–Dęblin 2015, s. 284–294; E. Lichocki, *Cyberterroryzm jako nowa forma zagrożeń dla bezpieczeństwa*, w: K. Liedel (red.), *Transsektorowe obszary bezpieczeństwa Narodowego*, Warszawa 2011, s. 16.

[176] Konkluzje Rady w sprawie Komisji i Wysokiego Przedstawiciela UE. Wspólna komunikacja Unii Europejskiej do spraw zagranicznych i polityki bezpieczeństwa w sprawie strategii cyberbezpieczeństwa Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, dok. 11357/13, Bruksela, 22 lipca 2013.

[177] C. Nosal, *Psychologia myślenia i działania menedżera*, Kraków 2001, s. 293.

[178] W. Łepkowski, *Podstawy strategii wojskowej*, Warszawa 2006, s. 46.

[179] J. Kubin, *Projektowanie strategii*, w: J. Kubin, Z. Żekoński (red.), *W poszukiwaniu strategii zmian*, Warszawa 1993, s. 142–143.
[180] W. Łepkowski, *Podstawy strategii*, s. 14.
[181] W. Nowicki, *Podstawy terminologii*, Warszawa 1986, s. 38.
[182] P. Soroka, *Polistrategia*, s. 220–230.
[183] W. Łepkowski, *Podstawy strategii*, s. 50; P. Soroka, *Polistrategia*, s. 260.
[184] R. Kuźniar, *Między polityką a strategią*, Warszawa 1994, s. 72.
[185] W. Pokruszyński, *Etymologia polityki i strategii bezpieczeństwa w świetle wyzwań i zagrożeń XXI wieku*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje" 2018, nr 22, s. 373–378.
[186] K. Loranty, *Bezpieczeństwo społeczne RP*, Warszawa 2004, s. 3–4.
[187] Zob.: P. Bączek, *Zagrożenie informacyjne*, s. 49.
[188] Por.: M. Tabor, *Polityka zagraniczna a tożsamość narodowa*, w: J. Kukułka, R. Zięba (red.), *Polityka zagraniczna państwa*, Warszawa 1992, s. 160.
[189] Szerzej: Z. Cesarz, E. Stadtmüller, *Problemy polityczne współczesnego świata*, Wrocław 1996, s. 229.
[190] W. Krztoń, *Walka o informację*, s. 102.
[191] COM(93) 0700 final.
[192] COM(96) 0389 final.
[193] Dokument dostępny na oficjalnej stronie internetowej KE w języku angielskim: http://europa.eu/rapid/press-release_IP-96-688_en.htm?locale=en (dostęp: 10.08.2020).
[194] Dokument dostępny na oficjalnej stronie internetowej Eur-Lex w języku angielskim: http://eurlex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24221 (dostęp:10.08.2020).
[195] R. Pałka, *Realizacja Strategii Lizbońskiej w latach 2000–2010 – zalecenia i rekomendacje, w tym dla Polski*, „Mazowsze. Studia Regionalne" 2011, nr 6, s. 12.
[196] J.S. Nowak, G. Bliźniuk (red.), *Społeczeństwo informacyjne*, s. 16.
[197] COM(2000) 0330 final.
[198] R. Zięba, *Unia Europejska jako aktor stosunków międzynarodowych*, Warszawa 2003, s. 264.
[199] COM(2002) 0263 final.
[200] COM(2007) 0267 final.
[201] Ramy unijnej polityki obrony cybernetycznej, Bruksela, 18 listopada 2014, s. 12, https://www.consilium.europa.eu/media/37024/st14413-en18.pdf (dostęp: 12.02.2020).
[202] https://eeas.europa.eu/top_stories/pdf/eugs_pl_.pdf. (dostęp: 13.08.2020).
[203] Por.: M. Wróblewska-Łysik, *Europejska Strategia Globalna a możliwości współpracy Unii Europejskiej z NATO po szczycie w Warszawie*, „Bezpieczeństwo Narodowe" 2016, nr I–IV, s. 67–70.
[204] S. Biscop, *The EU Global Strategy 2020*, „Security Policy Brief" 2019, nr 108, s. 1–3.

[205] Commission Staff Working Document Assessment of the EU 2013 Cybersecurity Strategy, 2017, źródło: https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF (dostęp: 18.04.2018).
[206] Ibidem.
[207] https://ec.europa.eu/poland/news/170919_cyber_attacks_pl (dostęp: 22.07.2019).
[208] COM(2017) 477.
[209] Ibidem.
[210] Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ENISA, „Agencji ds. Bezpieczeństwa cybernetycznego UE", uchylającego rozporządzenie (UE) 526/2013 oraz w sprawie certyfikacji cyberbezpieczeństwa technologii informacyjnych i komunikacyjnych („akt dotyczący cyberbezpieczeństwa"), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0477:FIN (dostęp: 19.04.2018).
[211] Dyrektywa Parlamentu Europejskiego i Rady 2016/1148/UE z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE UE L 194 z 19.07.2016).
[212] Szerzej: http://www.consilium.europa.eu/pl/policies/cyber-security/ (dostęp: 13.08.2018).
[213] https://ec.europa.eu/digital-single-market/en/cyber-security (dostęp: 13.08.2018).
[214] Ibidem.
[215] L.K. Ilves et al., *European Union and NATO Global Cybersecurity Challenges: A Way Forward*, „PRISM" 2016, vol. 6(2), s. 133.
[216] Ch. Garrison, C. Hamilton, *A comparative analysis of the EU GDPR to the US's breach notifications*, „Information & Communications Technology Law" 2019, vol. 28(1), s. 2.
[217] Regulation of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (EU) no 526/2013 (CYBERSECURITY ACT), Dok. PE-CONS 86/1/18 REV 1(2017/0225 (COD) LEX 1899).
[218] https://www.consilium.europa.eu/ (dostęp: 18.07.2020).
[219] *Biała Księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania* [COM(2020) 65 final].
[220] https://ec.europa.eu/digital-single-market/en/cyber-security (dostęp: 13.06.2020).
[221] J. Gryz, *Wzajemny związek*, s. 15.
[222] R. Kuźniar, *Europejska strategia*, s. 90.
[223] J. Gryz, *Bezpieczeństwo państwa władza – polityka – strategia*, Warszawa 2013, s. 74–80.

[224] Szerzej: I. Oleksiewicz, M. Górka, *Bezpieczeństwo pozamilitarne i quasi-militarne Europy Zachodniej*, Toruń 2019, s. 23–30.
[225] T. Aleksandrowicz, *Terroryzm międzynarodowy*, Warszawa 2008, s. 33–34.
[226] M. Abrahms, *What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy*, „International Security" 2008, nr 32, s. 88–90.
[227] *Słownik współczesnego języka polskiego*, t. I, Warszawa 1999, s. 701.
[228] *Uniwersalny słownik języka polskiego*, t. V, Warszawa 2003, s. 460.
[229] A. Markowski, *Nowy słownik poprawnej polszczyzny*, Warszawa 1999, s. 1277.
[230] P. Żmigrodzki, *Słownik synonimów i antonimów*, Wrocław 2007, s. 421.
[231] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008, s. 40.
[232] M. Frączek, *Bezpieczeństwo cyberprzestrzeni państwa – podstawowe problemy*, w: A. Polak, J. Lasota, M. Palczewska (red.), *Wojny i konflikty zbrojne XXI wieku – podejście polemologiczne*, Warszawa 2016, s. 284.
[233] T.R. Aleksandrowicz, K. Liedel, *Społeczeństwo informacyjne*, s. 16.
[234] M. Frączek, *Bezpieczeństwo cyberprzestrzeni*, s. 285.
[235] W.J. Lynn, N. Thompson, *The Pentagon's New Cyberstrategy*, Foreign Affairs, October 1, 2010, https://www.foreignaffairs.com/articles/2011-09-28/pentagons-cyberstrategy-one-year-later (dostęp: 14.07.2020).
[236] M. Łapczyński, *Zagrożenia cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*, https://pulaski.pl/wp-content/uploads/2015/02/Pulaski_Policy_Papers_No_7_09.pdf (dostęp: 14.07.2020).
[237] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 60.
[238] J. Janczak, G. Świdzikowski, *Bezpieczeństwo informacji w woskowym systemie telekomunikacyjnym*, Warszawa 2004, s. 43.
[239] P. Bączek, *Zagrożenia informacyjne*, s. 3–4.
[240] A. Lepa, *Świat manipulacji*, Częstochowa 1995, s. 157.
[241] M. Albahar, *Cyber Attacks and Terrorism: A Twenty-First Century Conundrum*, „Sci Eng Ethics" 2019, nr 25(4), s. 997.
[242] R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Warszawa 2011, s. 111113.
[243] Celem ataku jest zablokowanie serwera sieci komputerowej przy wykorzystaniu protokołu TCP, a jego rezultatem jest znaczne przeciążenie sieci komputerowej. Sposób ataku polega na wysyłaniu dużej liczby pakietów z odpowiednią w nagłówku flagą w synchronizacji (SYN) i zazwyczaj ze sfałszowanym adresem IP nadawcy w celu jego „zalania" dużą liczbą pakietów inicjujących połączenie.
[244] Celem ataku DoS jest uniemożliwienie działania sieci komputerowej i jej usług przez wykorzystanie do tego celu błędów w protokołach i aplikacjach. Sposób ataku polega na przeciążeniu aplikacji serwującej określone dane przez wysyłanie dużej liczby pakietów w celu wyczerpania zasobów systemu, by

doprowadzić do załamania pracy aplikacji. Inne metody to przeciążenie pracy łączy klientów o ograniczonej przepustowości do stanu, gdzie brak jest możliwości świadczenia usług oraz ograniczenie dostępu do zasobów komputerowych (pamięci operacyjnej, mocy obliczeniowej procesora, przestrzeni dyskowej). Rezultatem ataku jest załamanie pracy aplikacji świadczących usługi, blokowanie dostępu do zasobów sieci i usług, straty dla organizacji. DoS jest atakiem wykonanym z jednego komputera.

[245] Odmiana ataku DoS wykonana z kilkuset lub kilku tysięcy komputerów jednocześnie w celu wzmocnienia skuteczności ataku, czyli uniemożliwienia działania sieci komputerowej i jej usług. Atak rozpoczyna się z komputera klienta, który wysyła odpowiedni rozkaz do węzłów, te z kolei wysyłają go dalej do agentów, by przeprowadzić atak na ofiarę. Rezultatem jest załamanie pracy aplikacji świadczących usługi, blokowanie dostępu do zasobów sieci i usług z większą skutecznością niż atak DoS, znaczne straty i koszty dla organizacji. W ataku typu DDoS stosuje się zombie – komputer podłączony do Internetu z zainstalowanym oprogramowaniem umożliwiającym bez wiedzy jego użytkownika zdalne sterowanie z zewnątrz.

[246] DRDoS to jedna z nowszych odmian ataku DoS, którego celem jest uniemożliwienie dostępu do sieci komputerowej i jej usług. Przebieg ataku polega na generowaniu specjalnych pakietów SYN, których adres jest sfałszowany – jest nim adres ofiary. Duża liczba takich pakietów jest wysyłana do sieci. Komputery, do których one docierają, odpowiadają na adres pochodzący z fałszywego nagłówka. W ten sposób ofiara (zaatakowany komputer, system) otrzymuje wiele pakietów, w efekcie zostaje zablokowany i nie świadczy normalnych usług.

[247] Rodzaj ataku DoS na system komputerowy w celu jego zablokowania i uniemożliwienia świadczenia usług. Atak zakłada, że w środowisku rozproszonym – wieloprocesowym tylko część procesów może być uruchomiona równocześnie. Przebieg ataku to szybkie „rozmnożenie" kopii programu (aplikacji) w celu wypełnienia tablicy procesów systemu operacyjnego, tym samym jego zablokowanie, powstaje tzw. bomba. Wywołanie nowego procesu (np. w celu likwidacji procesu bomby) jest wstrzymane, ponieważ wymaga zwolnienia chociaż jednego z istniejących wpisów. Jest to mało prawdopodobne, gdyż każdy proces bomby jest w tym momencie gotowy się rozmnożyć. Rezultatem ataku jest zablokowany system, znaczne straty i koszty.

[248] J. Aycock, *Computer Viruses and Malware*, Calagary 2006, s. 245.

[249] A. Dawidczyk, *Nowe wyzwania, zagrożenia i szanse dla bezpieczeństwa Polski u progu XXI wieku*, Warszawa 2001, s. 48–49.

[250] J. Ching, *Cyberterrorism*, New York 2010, s. 56–58.

[251] D. Denning, *Is Cyber Terror Next?*, www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc (dostęp: 15.07.2020).

[252] Por.: D. Denning, *Cyberterrorism*, „Global Dialogue" Autumn 2000.

[253] Szerzej: K. Liedel, P. Piasecka, *Wojna cybernetyczna*, s. 18.

[254] W USA działań hakerskich nie traktuje się jako cyberterroryzmu, chyba że dokonywane są przez organizacje terrorystyczne. Próby uzyskania nieuprawnionego dostępu do sieci wojskowych czy rządowych, które mają na celu kradzież danych (tajnych informacji), powinniśmy raczej klasyfikować jako szpiegostwo niż sam akt cyberterroryzmu. Taka sama sytuacja dotyczy włamań do systemów bankowych, których celem jest opróżnienie kont. Tę działalność powinno się klasyfikować jako klasyczną działalność kryminalną, a nie jako cyberterroryzm. Szerzej: „e-Terroryzm.pl" 2012, nr 5, s. 8.

[255] A. Suchorzewska, *Ochrona prawna*, s. 17.

[256] D. Littlejohn Shinder, E. Tittel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Gliwice 2004, s. 25.

[257] D. Skowera, *Akademia Cyberpolicyjna – Policja i organizacje międzynarodowe wobec wyzwań przestępczości internetowej*, „Zarządzanie publiczne" Zeszyty Naukowe ISP UJ 2006, nr 2, s. 142. Por.: M. Depa, M. Pomykała, *Instytucjonalne aspekty przeciwdziałania cyberprzestępczości*, w: I. Oleksiewicz, M. Polinceusz, M. Pomykała (red.), *Nowoczesne technologie – źródło zagrożeń i narzędzie ochrony bezpieczeństwa*, Rzeszów 2014, s. 8.

[258] Por.: A. Becla, *Społeczeństwo informacyjne i społeczeństwo pseudoinformacyjne – problemy pojęciowe i metodyczne identyfikacji*, „Handel Wewnętrzny" 2012, t. 3, s. 151–153.

[259] Zob.: P. Daniluk, *Kultura strategiczna Unii Europejskiej. Podejście normatywne*, „Rocznik Bezpieczeństwa Międzynarodowego" 2015, t. 9(2), s. 14–17.

[260] A. Berlin, L. Brotherson, *Bezpieczeństwo defensywne. Podstawy i najlepsze praktyki*, Gliwice 2018, s. 73.

[261] V. Pitts, *Cyber Crimes: History of World's Worst Cyber Attacks*, Marousi 2017, s. 126.

[262] Zob.: M. Szczygieł, *Polityka cyberbezpieczeństwa Unii Europejskiej – początek drogi do strategicznej autonomii*, „Sprawy Międzynarodowe" 2018, nr 71(2), s. 161.

[263] Szerzej: M. Polinceusz, M. Pomykała, *Ochrona cyberbezpieczeństwa w Polsce. Kierunki zmian legislacyjnych na przestrzeni ostatnich lat*, w: P. Bogdalski i in. (red.), *Współczesne zagrożenia bioterrorystyczne i cyberterrorystyczne a bezpieczeństwo narodowe Polski*, Warszawa 2013, s. 660–661.

[264] W. Krztoń, *Walka o informację*, s. 145.

[265] J. Andersson et. al., *Envisioning European Defence: Five Futures*, „Chaillot Paper" 2017, nr 137, s. 122.

[266] Por.: orzeczenie Sądu Okręgowego w Paryżu z 20 października 2000 r. w sprawie Anit-Semitism LICRA v. Yahoo Inc., sygn. akt RG 00/05308.

[267] A. Adamski, *Cyberprzestępczość – aspekty*, s. 166.

[268] *Jak chińskie Politbiuro wojowało z Google*, http://www.tvn24.pl/wiadomosci-ze-swiata,2/jak-chinskie-politbiuro-wojowalo-z-google,154681.html (dostęp: 15.07.2017).

[269] Ransomware – złośliwe oprogramowanie, które szyfruje dane i blokuje do nich dostęp. Wszystkie komputery są zainfekowane w podobny sposób, a na ekranach każdego wyświetla się komunikat, w którym hakerzy domagają się okupu za odblokowanie sprzętu za pomocą bitcoinów.

[270] https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html (dostęp: 30.07.2020).

[271] K. Christensen, T. Liebetrau, *A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry*, „Intelligence and National Security" 2019, vol. 34(3), s. 399–400.

[272] Uważa się, że dokonano ok. 200 tys. ataków hakerskich w ciągu czterech dni. Szkody, jakie wyrządziły, szacuje się na ok. 8 mld dolarów.

[273] S. Haataja, *The 2007 Cyberattacks Against Estonia and International Law on the Use of Force: An Informational Approach*, „Law, Innovation and Technology" 2017, vol. 9, s. 159.

[274] D. Hollis, *Cyberwar Case Study: Georgia 2008*, „Small Wars Journal" 2011, http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf (dostęp: 12.04.2020).

[275] Ł. Czebotar, *Strategia Stanów Zjednoczonych wobec problemu bezpieczeństwa cyberprzestrzeni*, w: A. Podraza, P. Potakowski, K. Wiak (red.), *Cyberterroryzm zagrożeniem XXI wieku*, Warszawa 2013, s. 69.

[276] Y. Harrel, *Rosyjska cyberstrategia*, Warszawa 2015, s. 206–208.

[277] Ibidem, s. 201.

[278] M. Lakomy, *Unia Europejska wobec zagrożeń dla bezpieczeństwa teleinformatycznego – zarys problemu*, „Rocznik Integracji Europejskiej" 2013, nr 7, s. 130–132.

[279] F. Fukuyama, *Their target: The Modern Word*, „Newsweek" 17.12.2001.

[280] Szerzej: S.P. Huntington, *Zderzenie cywilizacji i nowy kształt ładu światowego*, Poznań 2018. Odmiennie: B. Barber*, Democracy and terror in the era of jihad vs. Mcworld*, w: K. Booth, T. Dunne (red.), *World in collision: terror and the future of global order*, New York 2002, s. 255–262.

[281] P. Mickiewicz, *System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, t. 11(1), s. 15.

[282] Por.: Z. Brzeziński, *O Polsce, Europie i Świecie 1988–2001*, Warszawa 2002, s. 313–315; J. Kukułka (red.), *Bezpieczeństwo międzynarodowe w Europie Środkowej po zimnej wojnie*, Warszawa 1994, s. 350–363; K. Żukrowska, *Globalizacja jako determinanta nowego systemu bezpieczeństwa międzynarodowego*, w: J. Osiński (red.), *Globalna gospodarka – lokalne społeczeństwa. Świat u progu XXI wieku*, Warszawa 2001, s. 245–262.

[283] A. Porębski, *Europejskie mniejszości etniczne. Geneza i kierunki przemian*, Kraków 1991, s. 62.

[284] R. Kupiecki, *Kultura strategiczna podmiotów zbiorowych. Przypadek NATO*, „Sprawy Międzynarodowe" 2017, nr 4, s. 17–20. Por.: A.M. Wilk, *Państwo w dobie społeczeństwa informacyjnego – perspektywa strategicznych zmian*, w: R. Skubisz (red.), *Internet 2000. Prawo – ekonomia – kultura*, Lublin 2000, s. 88.

[285] Por.: W. Gizicki, *Polityczne uwarunkowania*, s. 197–198.

[286] C. Jean, *Geopolityka*, Wrocław 2002, s. 246.

[287] Szerzej: A. Roberts, *Counter – terrorism, armed force and the laws of war*, „Survival" 2002, vol. 44, s. 7–32.

[288] M. Malinowski, R. Ożarowski, W. Grabowski, *Ewolucja terroryzmu na przełomie XX i XXI wieku*, Gdańsk 2009, s. 99–103.

[289] Jako przykład czasowej mobilizacji cyberterrorystów wskazać można apel imama Samudry z 2002 r., skierowany do młodych wyznawców islamu, nawołujący do prowadzenia dżihadu w cyberprzestrzeni przez atakowanie komputerów niewiernych i nielegalne wykorzystanie kart kredytowych, co pozwoliłoby na prowadzenie i finansowanie walki z Zachodem. Szerzej: B. Hołyst, *Terroryzm*, t. II, Warszawa 2011, s. 367.

[290] H. Wyrębek, P. Szmitkowski, *Koncepcja interaktywnego systemu ostrzegania i alarmowania ludności o zagrożeniach*, „Bezpieczeństwo i Technika Pożarnicza" 2018, vol. 50(2), s. 145.

[291] E. Lichocki, T. Mirosław, *Bezpieczeństwo sił zbrojnych RP w dobie zagrożeń cybernetycznych*, w: K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w dobie informacji*, Warszawa 2014, s. 140.

[292] S. Wojciechowski, *Reasons of Contemporary Terrorism. An Analysis of Main Determinants,* w: A. Sroka, F. Castro-Rial Garrone, R. Torres Kumbrian (red.), *Radicalism and Terrorism in the 21st Century*, Frankfurt am Main–Bern–Bruxelles–New York–Oxford–Warszawa–Wien 2017.

[293] A. Andrzejewska, *Cyberświat – możliwości i zagrożenia*, Warszawa 2009, s 24.

[294] Por. M. Wróblewska-Łysik, *Europejska Strategia Globalna a możliwości współpracy Unii Europejskiej z NATO po szczycie w Warszawie*, Warszawa 2016, s. 67–70.

[295] W. Barfield, *Cyber-Humans. Our Future with Machines*, New York 2015, s.19-21.

[296] U. Pagallo, *The laws of robots: crimes, contracts, and torts*, New York 2013, s. 47–66.

[297] Program sztokholmski – otwarta i bezpieczna Europa dla dobra i ochrony obywateli, Bruksela, 2 grudnia 2009 (17024/09); Przestrzeń wolności, bezpieczeństwa i sprawiedliwości: Plan działań służący realizacji programu sztokholmskiego (COM(2010) 171).

[298] Szerzej: rozdział 2.3.

[299] Obejmuje również: ochronę sieci i infrastruktury krytycznej, bezpieczeństwo granic zewnętrznych z budowaniem takich zdolności u swoich partnerów włącznie, ochronę cywilną i reagowanie na katastrofy, zapewnienie stabilnego

dostępu i korzystania z przestrzeni globalnych (cyberprzestrzeń, przeciwdziałanie zagrożeniom hybrydowym, cyberbezpieczeństwo, zapobieganie i przeciwdziałanie terroryzmowi zwalczanie przemytu, nielegalnej migracji oraz nielegalnego handlu bronią i zorganizowanej przestępczości). W ramach politycznej implementacji *Strategii globalnej* na szczególną uwagę zasługuje konsekwentne zmierzanie do uruchomienia PESCO, przewidzianej w art. 42.6 i 46 Traktatu o Unii Europejskiej i Protokole 10.

[300] COM(2016) 950 final, 30.11.2016.

[301] Commission Staff Working Document Assessment of the EU 2013 Cybersecurity Strategy, 2017, https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF (dostęp: 18.04.2018).

[302] Komunikat Komisji, *State of the Union 2017: The Commission scales up its response to cyberattacks,* 2017, źródło: europa.eu/rapid/press-release_MEMO-17-3194_en.pdf (dostęp: 19.04.2018).

[303] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, źródło: https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32016L1148&from=EN (dostęp: 19.04.2018).

[304] Por.: S. Kowalkowski (red.), *Niemilitarne zagrożenia bezpieczeństwa publicznego*, Warszawa 2011, s. 55.

[305] L.K. Ilves et al., *European Union*, s. 133.

[306] Mogą się w niej ścierać podmioty odległe od siebie o tysiące kilometrów. Przestrzeń teleinformatyczna ułatwiła ten proceder zarówno podmiotom państwowym, jak i pozapaństwowym. Obecnie, z drugiego końca globu, przy relatywnie niskim ryzyku poniesienia konsekwencji możliwe jest niemal błyskawiczne uzyskanie istotnych danych, w tym np. dokumentów i technologii o fundamentalnym znaczeniu dla bezpieczeństwa państwa.

[307] Szerzej: https://www.kaspersky.pl/ (dostęp: 27.05.2018).

[308] Szerzej: *APWG Phishing Activity Trends Report 4th Quarter of 2017*, http://www.apwg.org (dostęp: 27.05.2018).

[309] 70% trafia do właściciela strony, 30% do organizatorów procederu.

[310] Szerzej: https://www.pcformat.pl/News-Cryptojacking---to-nowa-forma-atatku,n,18068?utm_source=paste&utm_medium=paste&utm_campaign=firefox (dostęp: 27.05.2018).

[311] Państwa dość łatwo mogą wejść w posiadanie szkodliwego oprogramowania (wirusów, trojanów, robaków) i sprzętu potrzebnego do przeprowadzenia nawet zaawansowanych operacji. Agencje rządowe same opracowują coraz bardziej rozbudowane narzędzia, co nie wiąże się jednak z poważnymi kosztami z punktu widzenia budżetu (casus wirusa Stuxnet).

[312] A. Mazurkiewicz, *NATO and EU approach towards civil-military relations in militaryoperations*, „Polityka i Społeczeństwo" 2014, nr 2, s. 130.

[313] F. Schreier, *On cyberwarfare,* DCAF Horizon 2015, working paper, s. 7–10.

[314] Por.: I. Oleksiewicz, *Polskie prawo karne w zakresie walki z cyberprzestępczością na tle standardów prawa UE*, w: M. Pietraś, H. Chałupczak, J. Misiągiewicz (red.), *Europa Środkowo-Wschodnia w procesie transformacji i integracji. Wymiar bezpieczeństwa,* Zamość 2016, s. 530 i n.

[315] R. Zięba, *Unia Europejska*, s. 261.

[316] M. Czyżak, *Cyberprzestępczość a rozwój społeczeństwa informacyjnego*, „Ekonomiczne Problemy Usług" 2015, nr 117, s. 665.

[317] W literaturze przedmiotu można spotkać różne terminy odnoszone np. do sfery polityki zagranicznej i stosowane w naukach społecznych do opisywania związków przyczynowo-skutkowych. Ziemowit J. Pietraś używa terminu „wyznaczniki", który „oznacza […] zespół wzajemnie warunkujących się przesłanek powodujących określony skutek i wystarczających, aby dany skutek wystąpił" [Z.J. Pietraś, *Wyznaczniki polityki zagranicznej państwa*, w: A. Bodnar, J. Szczepański (red.), *Stosunki międzynarodowe. Problemy badań i teorii*, Warszawa 2007, s. 161. Zob. też: Z.J. Pietraś, *Podstawy teorii stosunków międzynarodowych*, Lublin 1986, s. 92]. Autor przytacza ponadto takie terminy, jak: przesłanki, czynniki, przyczyny, determinanty. Terminu „czynniki" używano, mówiąc o analizie czynnikowej jako jednej z metod badawczych w zakresie nauk społecznych (W. Kostecki, *Analiza czynnikowa stosunków międzynarodowych,* Warszawa 2015, s. 175). Remigiusz Bierzanek oraz Józef Kukułka także stosują termin „czynniki" (R. Bierzanek, *Współczesne stosunki międzynarodowe*, Warszawa 1972, s. 27–104; J. Kukułka, *Międzynarodowe stosunki polityczne*, Warszawa 1982, s. 79–92). Ryszard Zięba w odniesieniu do polityki zagranicznej posługuje się terminem „uwarunkowanie", który uważa za najszerszy, ponieważ obejmuje on czynniki warunkujące oraz oddziałujące w sposób bezpośredni, a zatem sprawcze – określające [R. Zięba, *Uwarunkowania polityki zagranicznej państwa*, w: R. Zięba (red.), *Wstęp do teorii polityki zagranicznej państwa*, Toruń 2005, s. 17]. Z kolei, mówiąc o ewolucji bezpieczeństwa państw, ten sam autor stosuje termin „czynniki" [R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego: koncepcje – struktury – funkcjonowanie*, Warszawa 2004, s. 36; por.: J. Zając, *Bezpieczeństwo państwa*, w: K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), *Bezpieczeństwo państwa: wybrane problemy*, Warszawa 2009, s. 19–20].

[318] Zob.: J. Kukułka, *Międzynarodowe stosunki*, s. 79–81.

[319] I. Oleksiewicz, R. Zacharski, I. Topolski, *Faces of the modern world. Political dimension*, Berlin 2018, s. 32–38.

[320] M. Brzeziński, *Podnoszenie poziomu ochrony obywateli i przedsiębiorstw w cyberprzestrzeni*, w: W. Fehler, K.P. Marczuk (red.), *Polityka Unii Europejskiej w zakresie bezpieczeństwa wewnętrznego*, Warszawa 2015, s. 80–81.

[321] D. Slater, *Socjal Relationships and Identity Online and Offline*, w: L. Lievrouw, S. Livingston (red.), *The Handbook of New Media*, London 2002, s. 355.

[322] K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011, s. 18.

[323] J. Domenach, *Europa: wyzwanie dla kultury*, Warszawa 1992, s. 69.
[324] Szerzej: B.M.J. Szewczyk, *Rozszerzenie i legitymacja Unii Europejskiej*, „Polski Rocznik Prawa Międzynarodowego" 2010, nr 30, s. 138–143.
[325] Por.: S. Wojciechowski, *Three dimensions of modern terrorism in the European Union*, „Rocznik Integracji Europejskiej" 2018, nr 12.
[326] M. Kopczewski*, Elementy infrastruktury krytycznej państwa, organizacji jako obiekty narażone na ataki cyberterrorystyczne*, Zakopane 2011, s. 582
[327] Interesującym przejawem tego typu działań były rosyjskie cyberataki na Estonię i Gruzję w latach 2007–2008. W obu przypadkach ograniczenie możliwości prowadzenia aktywnej polityki informacyjnej przez te państwa posłużyło wzmocnieniu pozycji Federacji Rosyjskiej na arenie międzynarodowej.
[328] T.R. Mockatis, *The New Terrorism: Myths and Realists*, „Stanford University Press" 2008, s. 29.
[329] J.R. Lup Jr, *Eschatology in a Secular Age: An Examination of the Use of Eschatology in the Philosophies of Heidegger, Berdyaev and Blumenberg*, Florida 2013, s. 49.
[330] B. Fijałkowska, A. Żukowski, *Unifikacja i zróżnicowanie się współczesnej Europy*, Warszawa 2002, s. 11.
[331] Por.: W. Krztoń, *Walka o informację*, s. 32.
[332] Por. J. Janowski, *Cybernetyzacja prawa*, w: E. Galewska, S. Kotecka (red.), *X-lecie CBKE. Księga pamiątkowa z okazji 10-lecia Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego*, Warszawa 2012, s. 143.
[333] S. Malešević, *Terrorism. In The Rise of Organised Brutality: A Historical Sociology of Violence*, Cambridge 2017, s. 12–19. Zob. też: M. Madej, *Instytucjonalizacja współpracy międzynarodowej w dziedzinie zwalczania terroryzmu w Europie*, w: R. Zięba (red.), *Instytucjonalizacja wielostronnej współpracy międzynarodowej w Europie*, S. Parzymies, Warszawa 2004, s. 397.
[334] D. Verton, *Black ice. Niewidzialna groźba cyberterroryzmu,* Katowice 2004, s.194.
[335] A. Rathmell, *Information warfare and sub-state actors: An organizational approach*, „Information, Communication and Society" 1998, vol. 1(4), s. 490.
[336] Problem ten przeanalizował również NCS (*National Communications System*), który w 2000 r. stwierdził, że „globalna zależność od połączonych ze sobą komputerów i słabości tego systemu sprzyja wzrostowi zagrożenia cyberterroryzmem". Ponadto kierunek ewolucji grup terrorystycznych czyni je szczególnie dostosowanymi do wykorzystania Internetu w realizacji swoich celów. Wiele grup terrorystycznych przeszło ewolucję od struktur silnie hierarchicznych z określonymi przywódcami na czele do stowarzyszeń o dość luźnych powiązanych między częściowo niezależnymi komórkami, bez wyraźnej hierarchii – jak Hamas i organizacja bin Ladena. Szerzej: F. Jasiński, P. Rakowiecki, *Unia Europejska wobec walki z terroryzmem*, w: A. Górski, A. Sakowicz

(red.), *Zwalczanie przestępczości w Unii Europejskiej. Współpraca sądowa i policyjna w sprawach karnych*, Warszawa 2006.

[337] S. Jaskuła, *Informacyjna przestrzeń*, s. 198.

[338] E. Cała-Wacinkiewicz i in., *System Narodów Zjednoczonych z polskiej perspektywy*, Warszawa 2018, s. 359.

[339] Statut Rady Europy, przyjęty w Londynie dnia 5 maja 1949 r. (Dz.U. z 1994 r. Nr 118, poz. 565).

[340] Budapeszt 23.11.2001 r., CETS nr 185. Konwencja powstała pod koniec lat 90. XX w., a została otwarta do ratyfikacji 23 listopada 2001 r. w Budapeszcie. Polska podpisała wówczas tę konwencję, lecz dzisiaj jeszcze jej nie ratyfikowała.

[341] Szerzej: R. Tarnogórski, *Konwencja o cyberprzestępczości – międzynarodowa odpowiedź na przestępczość ery informacyjnej*, w: M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa Polski*, Warszawa 2009, s. 205–206.

[342] F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 163.

[343] Ibidem, s. 165.

[344] P. Gulda, *Internet a prawa człowieka*, „Gdańskie Studia Prawnicze" 2005, nr 13, s. 219. Zob. też: I. Oleksiewicz, *Cyberterroryzm – jako przykład łamania prawa godności człowieka*, w: T. Jemioła, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm nowe wyzwania XXI wieku*, Warszawa 2009, s. 437–451.

[345] Por.: sprawa Irlandia v. Wielka Brytania, 18.01.1978; sprawa Soering v. Wielka Brytania, 07.07.1989; sprawa Clauhal v. Wielka Brytania, 15.11.1966; sprawa Aksoy v. Turcja, 18.12.1966; sprawa Tomasi v. Francja, 27.08.1992.

[346] Zob.: H. Cornwall, *Datatheft*, s. 8.

[347] Rzeczpospolita Polska podpisała go w 21 lipca 2003 r., a ratyfikowała razem z Konwencją Rady Europy o cyberprzestępczości (Dz.U. z 2015 r. poz. 730).

[348] Lanzarote, 25 października 2007 r., CETS nr 201. Polska podpisała konwencję 25 października 2007 r., jednak jej nie ratyfikowała.

[349] Por.: A. Grzelak, M. Królikowski (red.), A. Sakowicz, *Europejskie prawo karne 2012*, Warszawa 2012, s. 276.

[350] A. Gajda, *Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomiczno-Społecznego Studia i Prace. Szkoła Główna Handlowa" 2014, nr 4, s. 2.

[351] J. Barta, R. Markiewicz, *Ochrona danych osobowych*. *Komentarz*, Kraków 2001, s. 39.

[352] *Podręcznik europejskiego prawa o ochronie danych*, Agencja Praw Podstawowych Unii Europejskiej 2014, Rada Europy 2014, Luksemburg: Urząd Publikacji Unii Europejskiej 2014 r., s. 16 źródło: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ae65e (dostęp: 27.07.2020).

[353] Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie 4 listopada 1950 r., zmieniona następnie Protokołami 3,

5 i 8 oraz uzupełnioną Protokołem 2 (Dz.U. z 1993 r. nr 61, poz. 284 ze zm.).

[354] A. Grzelak, *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości. W stronę standardu europejskiego*, Warszawa 2015, s. 143.

[355] Por.: J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2011, s. 46.

[356] A. Grzelak*, Ochrona danych*, s. 145.

[357] Przekład w: T. Jasudowicz, *Ochrona danych osobowych. Standardy europejskie. Zbiór materiałów*, Toruń 1998, s. 71.

[358] Por.: M. Ciechomska, *Zmiana Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych szansą na powstanie globalnego instrumentu ochrony danych*, „Monitor Prawniczy" 2017, nr 25(16), s. 871877.

[359] Zmiany Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (ETS nr 108) pozwalające na przystąpienie Wspólnot Europejskich, przyjęte przez Komitet Ministrów w Strasburgu w dniu 15 czerwca 1999 r., art. 23 ust. 2 Konwencji nr 108 w nowym brzmieniu.

[360] Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych sporządzony w Strasburgu 8.11.2001 r. (Dz.U. z 2006 r. Nr 3, poz. 15).

[361] https://www.interpol.int/Who-we-are/What-is-INTERPOL (dostęp: 30.07.2020).

[362] Utworzona na podstawie Rezolucji Zgromadzenia Ogólnego Interpolu nr AG-2008-RES-07 Poszerzenie systemu komunikacji I-24/7 do jednostek cybercrime w celu ułatwienia wymiany aktualnych informacji.

[363] J. Kosiński, *Działania terrorystyczne a cyberprzestępczość*, w: J. Szafrański, J. Kosiński (red.), *Współczesne zagrożenia terrorystyczne oraz metody ich zwalczania. Materiały pokonferencyjne*, Szczytno 2007, s. 238.

[364] T. Safjański, *Prawne aspekty wykorzystania wsparcia Interpolu w poszukiwaniu osób podejrzanych w świetle art. 605a k.p.k.*, „Prokuratura i Prawo" 2016, s. 155 i n.

[365] https://www.interpol.int/News-and-Events/News/2014/INTERPOL-Global-Complex-for-Innovation-opens-its-doors (dostęp: 30.07.2020).

[366] Dotyczy to zwłaszcza celu 16 (SDGs 16) „Pokój, sprawiedliwość i silne instytucje", który wyznacza cele w zakresie ograniczenia wszelkich form przemocy, ograniczenia handlu bronią i walki z przestępczością zorganizowaną.

[367] M. Smarzewski, *Cyberterroryzm a cyberprzestępstwa o charakterze terrorystycznym*, „IUS NOVUM" 2017, nr 1, s. 65.

[368] Szerzej: K. Dudka (red.), *Kodeks postępowania karnego. Komentarz*, Warszawa 2018, s. 489.

[369] *Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami. Analiza sytuacji i rekomendacje działań*, „Cyfrowa Polska",

Warszawa 2019, s. 4–5.

[370] Rezolucja przyjęta przez Sekretarza Generalnego w dniu 21 grudnia 1990 r. (A/RES/45/239).

[371] https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpiecze%C5%84stwo-A.D.-2018.pdf, s. 39 (dostęp: 23.07.2020).

[372] Szerzej: *International review of criminal Policy*. 1994, No. 43–44 (UN. Centre for Social Development and Humanitarian Affairs).

[373] https://www.itu.int/en/Pages/default.aspx (dostęp: 30.07.2020).

[374] Konwencja wiedeńska z 11 kwietnia 1980 r. weszła w życie 1 stycznia 1988 r. Obecnej jej stronami jest 85 państw, w tym Polska.

[375] Dz.U. z 2005 r. nr 18, poz. 158.

[376] Rezolucja przyjęta przez Sekretarza Generalnego 27 grudnia 2013 r. (A/RES/53/70).

[377] Rezolucja Rady Gospodarczej i Społecznej ONZ przyjęta w lipcu 2011 r. (E/2011/30).

[378] K. Lankosz (red.), *Traktat o Unii Europejskiej – komentarz*, Warszawa 2003, s. 428–429.

[379] Dz.Urz. WE C 187 z 3.07.2001.

[380] Dz.Urz. WE C 408 z 13.12.1998.

[381] W. Czapliński, C. Mik, *Traktat o Unii Europejskiej. Komentarz*, Warszawa 2005, t. 1, s. 579.

[382] F. Jasiński, P. Rakowiecki, *Unia Europejska wobec walki z terroryzmem*, w: A. Górski, A. Sakowicz (red.), *Zwalczanie przestępczości w Unii Europejskiej. Współpraca sądowa i policyjna w sprawach karnych*, Warszawa 2006, s. 156–158.

[383] Ibidem, s. 63. Zob. też: K. Kasowska-Pedrycz, *Polityka bezpieczeństwa wewnętrznego UE – ewolucja i perspektywy*, w: R. Bäcker, J. Marszałek-Kawa, J. Modrzyńska (red.), *Od starej do nowej Europy?*, Toruń 2005.

[384] Z. Brodecki, *Komentarz do Traktatu o Unii Europejskiej sporządzonego w Maastricht dnia 7 lutego 1992 r.,* w: *Traktat o Unii Europejskiej, Traktat ustanawiający Wspólnotę Europejską z komentarzem*, Warszawa 2006, s. 153.

[385] Zob.: sprawa Ergi vs. Turcja, 28.07.1998 r.; Raport Komisji z dnia 20 maja 1997 r.; K. Lankosz (red.), *Traktat o Unii Europejskiej*, s. 181–182.

[386] Wspólne działanie z 15 października 1996 r. przyjęte przez Radę na podstawie art. K.3 Traktatu o Unii Europejskiej, dotyczące utworzenia i utrzymywania spisu na temat szczególnych uprawnień antyterrorystycznych, umiejętności i wiedzy specjalistycznej ułatwiających współpracę antyterrorystyczną między państwami członkowskimi Unii Europejskiej (Dz.Urz. WE L 273 z 25.10.1996); Wspólne działanie z 21 grudnia 1998 r. przyjęte przez Radę na podstawie art. K.3 Traktatu o Unii Europejskiej, w sprawie uznawania za przestępstwa karne uczestnictwa w organizacji przestępczej w państwach członkowskich Unii Europejskiej (Dz.Urz. WE L 351 z 29.12.1998).

[387] K. Lankosz (red.), *Traktat o Unii Europejskiej*, s. 439.

[388] Por.: P. Wawrzyk, *Bezpieczeństwo wewnętrzne Unii Europejskiej*, Warszawa 2009, s. 64.
[389] Ibidem, s. 76–77.
[390] Dz.Urz. UE C 340 z 10.11.1997.
[391] Por.: M. Madej, *Instytucjonalizacja*, s. 235–263.
[392] A. Adamski, *Cyberprzestępczość – rozwój regulacji prawnej w Europie. Doświadczenia krajowe na tle implementacji prawnych instrumentów zwalczania cyberprzestępczości*, „Prokuratura i Prawo" 2011, nr 6, s. 174.
[393] K. Jałoszyński, *Współczesny wymiar antyterroryzmu*, Warszawa 2008, s. 32–65.
[394] W. Czapliński, *Wprowadzenie do prawa Unii i Wspólnot*, Kraków 2002, s. 55–56.
[395] A. Kańciak, *Unia Europejska na drodze do zwiększenia ochrony cyberprzestrzeni. Wybrane zagadnienia prawne*, „Studia Prawnoustrojowe" 2017, nr 38, s. 57.
[396] M. Kula i in., *Zwalczanie przestępczości w Unii Europejskiej. Współpraca sądowa i policyjna w sprawach karnych*, Warszawa 2006, s. 400 i n.
[397] P.J. Borkowski, *Polityczne teorie integracji międzynarodowej*, Warszawa 2007, s. 435.
[398] Obowiązkowy termin sześciu tygodni między momentem złożenia propozycji a wpisaniem jej do porządku obrad Rady.
[399] J. Węc, *Ewolucja wymiaru sprawiedliwości i spraw wewnętrznych Unii Europejskiej w latach 1992–2001*, „Zeszyt Naukowy" 2010, nr 4, s. 11–20.
[400] A. Gruszczak, *Eurojust i jego miejsce w europejskiej współpracy sądowej*, „Państwo i Prawo" 2003, nr 4, s. 76–78.
[401] G. Balawajder, *Instytucjonalny wymiar ochrony granic zewnętrznych Unii Europejskiej w kontekście bezpieczeństwa państw członkowskich*, „Pogranicze. Polish Borderlands Studies" 2018, vol. 6(1), s. 80.
[402] Porównaj np. orzeczenia ETS w sprawach C-496/19 – wyrok TS z 16.07.2020 r.; C-558/18 – wyrok TS z 26.03.2020 r.; C-274/14 – wyrok TS z 21.01.2020 r.
[403] K. Lankosz (red.), *Traktat o Unii Europejskiej*, s. 438.
[404] A. Gruszczak, *Wzmocniona współpraca w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych Unii Europejskiej*, „Studia Europejskie" 2002, nr 2, s. 96–97.
[405] Szerzej: J. Barcz (red.), *Prawo Unii Europejskiej. Zagadnienia systemowe*, Warszawa 2002, s. 121.
[406] Por.: P. Wawrzyk, *Bezpieczeństwo*, s. 72.
[407] Dz.Urz. UE C 80 z 10.3.2001; Dz.Urz. UE C 325 z 24.12.2002.
[408] Por.: S. Biscop, *The EU*, s. 7. Zob. też: F. Jasiński, M. Narojek, P. Rakowski, *Strategia antyterrorystyczna Unii Europejskiej*, „Wspólnoty Europejskie" 2006, nr 1, s. 47.
[409] Decyzja Rady 2002/187/WSiSW z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością (Dz.Urz. UE L 63 z 06.03.2002).
[410] Warunki, jakie dodał TN, były następujące: 1) nie mogła ona naruszać zasad rynku wewnętrznego ani spójności gospodarczej i społecznej; 2) nie mogła

stanowić dyskryminacji czy przeszkody w wymianie handlowej między państwami członkowskimi, nie mogła również powodować żadnego zniekształcenia warunków konkurencji UE; 3) musiała obejmować co najmniej osiem państw członkowskich; 4) nie mogła naruszać przepisów Protokołu acquis Schengen.

[411] Zob.: A. Gruszczak, *Eurojust*, s. 78.

[412] Proposal for a Council regulation amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (COM(2002) 406 – C5-0433/2002 – 2002/0173(CNS)). Zob. też: G. Stronikowska, *Prokuratura Europejska jako instytucja ochrony interesów finansowych Unii Europejskiej*, Warszawa 2020, s. 256.

[413] Por.: sprawa Fox, Campbell i Chartley v. Wielka Brytania, 30.08.1990 r.; sprawa Murray v. Wielka Brytania, 28.10.1994 r.

[414] Decyzja Komitetu Stałych Przedstawicieli z dnia 13 czerwca 2001 r. ustanawiająca grupę roboczą wysokiego szczebla (Dz.Urz.WE C z 29.06.2001).

[415] W dziedzinach objętych niniejszym tytułem państwa członkowskie wzajemnie się informują i konsultują ze sobą w ramach Rady, mając na względzie koordynację swoich działań. W tym celu ustanawiają współpracę między swoimi właściwymi jednostkami administracyjnymi.

[416] *Komisja podejmuje kroki w celu wzmocnienia współpracy UE w walce z terroryzmem, przestępczością zorganizowaną i cyberprzestępczością, 2015*, źródło: europa.eu/rapid/press-release_IP-15-4865_en.pdf. (dostęp: 2.07.2020).

[417] Szerzej: J. Barcz (red.), *Prawo Unii*, s. 23–45.

[418] Szerzej: P. Wawrzyk, *Bezpieczeństwo*, s. 88.

[419] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Zamknięcie obiegu plan działania UE dotyczący gospodarki o obiegu zamkniętym*, źródło: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52015DC0614 (dostęp: 12.07.2019).

[420] P. Zherestov, *From visible pasts to an invisible presence: New criminological reality after planetary cyberattack 12/05/17 Wannacry*, „Przegląd Wschodnioeuropejski" 2018, nr 2, s. 55–67; K. Kjærgaard-Christensen, T. Liebetrau, *A new role*, s. 399–400.

[421] M. Madej, *Instytucjonalizacja*, s. 239.

[422] K. Lankosz (red.), *Traktat o Unii Europejskiej*, s. 428–429.

[423] – pogłębianie międzynarodowego konsensusu i wzrost wysiłków społeczności międzynarodowej związanej z walką z terroryzmem,
– ograniczenie dostępu terrorystów do i finansowych i środków gospodarczych,
– rozwój instrumentów instytucji UE i państw członkowskich wcelu zidentyfikowania terrorystów, ścigania i zapobiegania atakom terrorystycznym,
– zapewnienie bezpieczeństwa transportu międzynarodowego i skuteczności systemu kontroli granicznej,

– rozwijanie umiejętności Unii Europejskiej i państw członkowskich w zakresie radzenia sobie z konsekwencjami ataku terrorystycznego,
– znajdowanie czynników, które przyczyniają się do terroryzmu,
– działania docelowe w stosunkach zewnętrznych UE z państwami trzecimi, których zdolność do walki z terroryzmem musi być wzmocniona.

[424] Por.: A. Grzelak, *Traktat formujący UE – proponowane zmiany w dziedzinie Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości UE*, w: J. Barcz (red.), *Traktat reformujący Unię Europejską*, „Koźmiński Law School Papers" 2007, nr 5, s. 86–97.

[425] Decyzję upoważniającą do podjęcia wzmocnionej współpracy RE przyjmuje w ostateczności, jeżeli ustali, że cele takiej współpracy nie mogą zostać osiągnięte w rozsądnym terminie przez Unię jako całość, oraz pod warunkiem, że uczestniczy w niej co najmniej dziewięć państw członkowskich. Rada stanowi zgodnie z procedurą określoną w art. 329 Traktatu o funkcjonowaniu Unii Europejskiej. W obradach Rady mogą uczestniczyć wszystkie państwa członkowskie, jednak w głosowaniu biorą udział tylko członkowie Rady reprezentujący państwa członkowskie uczestniczące we wzmocnionej współpracy. Zasady głosowania są przewidziane w art. 330 Traktatu o funkcjonowaniu Unii Europejskiej. Akty przyjmowane w ramach wzmocnionej współpracy wiążą wyłącznie uczestniczące państwa członkowskie. Nie są one uważane za dorobek, który musi zostać przyjęty przez państwa kandydujące do przystąpienia do Unii.

[426] P. de Wilde, A. Leupold, H. Schmidtke, *Introduction: The Differentiated Politicisation of European Governance*, „West European Politics" 2016, vol. 39(1).

[427] Zob.: J. Barcz, *Przewodnik po Traktacie z Lizbony. Traktaty ustanawiające Unię Europejską*, Warszawa 2008, s. 63–75.

[428] Decyzji nie należy tu rozumieć zbyt formalnie, tj. w takim znaczeniu, w jakim to pojęcie występuje w art. 249 TWE. Wydaje się, że tak określona kompetencja stanowi ogólną podstawę wykonywania przez nie kompetencji prawodawczej. Zob.: K. Lankosz, M. Szczygieł (red.), *Polityka cyberbezpieczeństwa Unii Europejskiej – początek drogi do strategicznej autonomii*, „Sprawy Międzynarodowe" 2018, nr 2.

[429] Zob.: H.V. Milner, *The Digital Divide – The role of political institutions in Technology Diffusion*, „Comparative Political Studies" 2006, vol. 39(2), s. 135.

[430] Por.: P. Craig, G. de Burca, *EU Law. Text, Cases and Materials*, Oxford 2003, s. 146–147.

[431] Ten zapis najbardziej przypomina dotychczasowe art. 60 i art. 301 TWE, jednak w tym wypadku zmianie uległa także procedura podejmowania decyzji. Jest również przedmiotem rozporządzenia Rady (WE) nr 2580/2001 z dnia 27 grudnia 2001 r. w sprawie szczególnych środków restrykcyjnych skierowanych przeciwko niektórym osobom i podmiotom mającym na celu zwalczanie terroryzm (Dz.Urz. WE L 344 z 28.12.2001).

[432] Oprócz zmiany nazwy z Komitetu Koordynacyjnego na Stały Komitet ds. Zapewnienia Wspierania i Wzmacniania Współpracy Operacyjnej Wewnątrz Unii zmieniono przede wszystkim zakres zadań tego organu, zawężając je do czynności jedynie operacyjnych, a tym samym współpracy w ramach policji.
[433] Zob.: wyrok w sprawie C-176/03 Komisja v. Rada, a także sprawie C-440/05 Komisja v. Rada.
[434] A. Grzelak, *Traktat formujący UE*, s. 39.
[435] Wyrok z 3.06.2007 r. w sprawie C-303/05, Advocaten voor de Wereld v. Leden.
[436] J. Barcz (red.), *Traktat z Lizbony. Główne reformy ustrojowe Unii Europejskiej*, Warszawa 2008, s. 45–48.
[437] Zob.: M. Szwarc-Kuczer, *Harmonizacja znamion przestępstw i kar w Traktacie z Lizbony,* „Europejski Przegląd Sądowy" 2009, nr 4, s. 10–17.
[438] Por.: B. Bieniek, *Pranie pieniędzy w prawie międzynarodowym, europejskim oraz polskim*, Warszawa 2010, s. 196.
[439] Szerzej: M. Szwarc-Kuczer, *Harmonizacja znamion*, s. 27.
[440] Zob.: Ł. Krysiński, *Identyfikacja cyberprzestępców*, „Państwo i Prawo" 2020, nr 2, s. 20.
[441] Zadania te mogą obejmować: a) wszczynanie śledztwa karnego oraz występowanie z wnioskiem o wszczęcie ścigania prowadzonego przez właściwe organy państwowe, w szczególności dotyczące przestępstw przeciwko interesom finansowym Unii; b) koordynację śledztw i ścigania, o których mowa w lit. a); c) wzmacnianie współpracy sądowej, w tym przez rozstrzyganie sporów o właściwość i ścisłą współpracę z Europejską Siecią Sądową.
[442] Por.: P. Opitek, *Skimming – aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej*, Warszawa 2017, s. 458–460.
[443] Zadania te mogą obejmować: a) gromadzenie, przechowywanie, przetwarzanie, analizę i wymianę informacji przekazywanych zwłaszcza przez organy państw członkowskich, państw trzecich lub instytucji spoza UE; b) koordynowanie, organizowanie i prowadzenie dochodzeń i działań operacyjnych prowadzonych wspólnie z właściwymi organami państw członkowskich lub w ramach wspólnych zespołów dochodzeniowych, w stosownych przypadkach w powiązaniu z Eurojustem.
[444] K. Oppermann, The Politics of Avoiding Referendums on the Treaty of Lisbon, „Journal of European Integration" 2013, vol. 35(1), s. 73–89.
[445] W. Wessels, *The Maastricht*, s. 753–767.
[446] B.M.J. Szewczyk, *Rozszerzenie*, s. 138–143.
[447] W. Kapica (red.), *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa 2020, s. 84.
[448] R. Zięba, *Wspólna polityka zagraniczna i bezpieczeństwa Unii Europejskiej*, Warszawa 2007, s. 88. Klauzule UE o wzajemnej obronie i solidarności: wymiar polityczny i operacyjny (Dz.Urz. UE C 419/138 z 16.12.2015), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52012IP0456 (dostęp: 2.07.2019).

[449] Dz.Urz. WE L 281 z 23.11.1995.
[450] Dz.Urz. WE L 178 z 17.07.2000.
[451] Dz.Urz. UE L 108 z 24.04.2002.
[452] Ibidem.
[453] Dz.Urz. UE L 201 z 31.07.2002.
[454] Dz.Urz. UE L 69 z 16.03.2005.
[455] Dz.Urz. UE L 345 z 23.12.2008.
[456] Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.Urz. UE L 335 z 17.12.2011).
[457] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. UE L 218 z 14.08.2013).
[458] Dz.Urz. UE L 130 z 01.05.2014.
[459] Dz.Urz. UE L 201 z 31.07.2002.
[460] Szerzej: A. Suchorzewka, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, Warszawa 2012, s. 162.
[461] Dz.Urz. UE L 201 z 31.07.2002.
[462] Dz.Urz. UE L 69 z 16.03.2005.
[463] Dz.Urz. UE L 77 z 13.03.2004.
[464] Dz.Urz. UE L 108 z 24.04.2002.
[465] Ibidem.
[466] A. Żebrowski, *Walka informacyjna na służbie terrorystów*, cz.1, „e-Terroryzm.pl" 2014, nr 2, s. 7.
[467] T.R. Aleksandrowicz, *Sieciowy paradygmat*, s. 165.
[468] A. Wąsek, R. Zawłocki, *Komentarz do rozdziału XXXIII KK Przestępstwa przeciwko ochronie informacji*, w: A. Wąsek, R. Zawłocki (red.), *Komentarz do kodeksu karnego. Część szczególna*, t. II, Warszawa 2010, s. 570–580; K. Lewandowski, *Przestępstwa przeciwko ochronie informacji w świetle Rozdziału XXXIII kodeksu karnego, orzecznictwa i doktryny*, „Wojskowy Przegląd Prawniczy" 2010, nr 3, s. 61 i n.
[469] Agencja składa się z Zarządu, Dyrektora Naczelnego, który nią zarządza, oraz Stałej Grupy Udziałowców złożonej z ekspertów reprezentujących właściwych udziałowców, takich jak przemysł technologii informacyjnych i łączności, grupy konsumenckie oraz ekspertów akademickich w zakresie bezpieczeństwa sieci i informacji. W skład Zarządu wchodzi jeden przedstawiciel każdego z państw członkowskich, trzech przedstawicieli wyznaczonych przez Komisję oraz trzech przedstawicieli bez prawa głosowania, zaproponowanych przez Komisję i wyznaczonych przez Radę. Zarząd określa ogólną orientację działania Agencji i zapewnia jej funkcjonowanie zgodnie z zasadami określonymi w rozporządzeniu. Zarząd gwarantuje również spójność pracy Agencji z działaniami państw członkowskich i Wspólnoty. Por.: K. Jałoszyński,

T. Aleksandrowicz, K. Wiciak, *Bezpieczeństwo państwa a zagrożenie terroryzmem. Instytucje państwa wobec zagrożenia terroryzmem*, t. II, Szczytno 2016; T. Przesławski, *Cel w konstrukcji przestępstwa terrorystycznego*, „Prokuratura i Prawo" 2009, nr 5, s. 18.

[470] Szerzej: D. Adamski, *Europejskie prawo łączności elektronicznej – telefonia, telewizja, Internet*, Warszawa 2005, s. 43; I. Oleksiewicz, *Ustawodawstwo polskie wobec przestępstwa o charakterze terrorystycznym*, w: Z. Nowakowski i in. (red.), *Wspólna polityka bezpieczeństwa i obronności. Implikacja dla Polski*, Warszawa 2011, s. 633–653.

[471] K. Ficoń, *Bezpieczeństwo*, Warszawa 2013, s. 157.

[472] Dz.Urz. UE L 345 z 23.12.2008.

[473] A. Adamski, *Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę*, w: G. Szpor (red.), *Internet. Ochrona wolności własności i bezpieczeństwa*, Warszawa 2011, s. 345–350.

[474] K. Lankosz, M. Chorośnicki, P. Czubik (red.), *Walka z terroryzmem międzynarodowym w świetle prawa międzynarodowego*, Bielsko-Biała 2004.

[475] M. Chorośnicki, *Czas strachu. Terroryzm – Europa – Polska*, Warszawa 2015, s. 76.

[476] Por.: K. Liedel, P. Piasecka, *Terroryzm wczoraj i dziś*, Warszawa 2015, s. 98; K. Boratyńska et. al., *Zwalczanie przestępczości w Unii Europejskiej. Współpraca sądowa i policyjna w sprawach karnych*, Warszawa 2006, s. 78–79.

[477] Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.Urz. UE L 335 z 17.12.2011).

[478] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. UE L 218 z 14.08.2013).

[479] Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz.Urz. UE L 69 z 16.03.2005).

[480] Szerzej: Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 4 lipca 2013 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową Rady 2005/222/WSISW (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)). Zob.: A.M. Kruk, *Bezpieczeństwo transferu informacji w XXI wieku w świetle bezpieczeństwa państwa i organizacji*, w: S. Sulowski, M. Brzeziński (red.), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Warszawa 2009, s. 345.

[481] A. Lasota, *Cyberatak jako wstęp do cyberwojny*, „Studia Mazowieckie" 2014, nr 4. Por.: K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015, s. 139.

[482] F. Radoniewicz, *Odpowiedzialność karna*, s. 229; F. Radoniewicz, *Postanowienia decyzji ramowej Rady w sprawie ataków na systemy informatyczne a*

ujęcie cyberprzestępstw w kodeksie karnym, „Ius Novum" 2009, nr 1, s. 48.

[483] Art. 10 dyrektywy. Zob.: K. Indecki, *Prawo karne wobec terroryzmu i aktu terrorystycznego*, Łódź 1998; R. Zgorzały, *Przestępstwo o charakterze terrorystycznym w polskim prawie karnym*, „Prokuratura i Prawo" 2007, nr 7–8; I. Oleksiewicz, *Podstawy prawne współpracy karnej i policyjnej Unii Europejskiej w ramach polityki antyterrorystycznej Unii Europejskiej,* w: I. Oleksiewicz, M. Pomykała, J. Rajchel (red.), *Współpraca instytucjonalna w Unii*, Rzeszów 2010, s. 33–50.

[484] Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.Urz. UE L 335 z 17.12.2011).

[485] IP/10/1535 i MEMO/10/598.

[486] Przyjęta jeszcze w 2006 r. Strategia UE na rzecz bezpiecznego społeczeństwa informacyjnego w Europie zwracała uwagę na problem cyberterroryzmu. Podkreślała, że ataki skierowane na prywatne lub rządowe systemy informatyczne w państwach członkowskich UE nadały mu nowy wymiar, jako potencjalnej nowej broni ekonomicznej, politycznej i wojskowej. Sugerowała, że w tym obszarze konieczne są dalsze prace w celu podniesienia poziomu świadomości i zacieśnienia współpracy unijnej. Szerzej: I. Oleksiewicz, *Polityka antyterrorystyczna Unii Europejskiej*, Lublin 2013, s. 28.

[487] Dz.Urz. UE L 130 z 01.05.2014.

[488] Dz.Urz. UE L 350 z 30.12.2008.

[489] Organem wykonującym jest organ właściwy do uznania END i zapewnienia jego wykonania zgodnie z niniejszą dyrektywą oraz z procedurami mającymi zastosowanie w podobnych sprawach krajowych.

[490] Oznacza państwo członkowskie, w którym wydawany jest END (art. 2 ust. 1 lit. a). Por.: K. Dudka (red.), *Kodeks postępowania*, s. 679.

[491] Oznacza państwo członkowskie wykonujące END, w którym ma zostać przeprowadzona dana czynność dochodzeniowa (art. 2 ust. 1 lit. b).

[492] *N. Catelan, S. Cimamonti, J.B. Perrier, La luttecontre le terrorismedans le droit et la jurisprudence de l`Unioneuropeenne*, Marseille 2014. Szerzej: D. Świecki (red.), *Kodeks postępowania karnego. Komentarz*, t. II, Warszawa 2018, s. 376.

[493] I. Oleksiewicz, *Challenges of EU security on the example of cyberrorism policy*, „Journal of International Trade Law of Policy" 2015, nr 1, s. 34–35.

[494] Dz.Urz. UE L 194 z 6.07.2016.

[495] Dyrektywa określa, jakim obowiązkom z zakresu bezpieczeństwa będą podlegać operatorzy usług kluczowych (sektory krytyczne, np. energetyka, transport, opieka zdrowotna i finanse) oraz dostawcy usług cyfrowych (internetowe platformy handlowe, wyszukiwarki, usługi przetwarzania w chmurze). Dyrektywa wymaga, by każdy kraj UE posiadał strategię bezpieczeństwa sieci i informacji. Choć Polska posiada bardzo ważny dokument poświęcony cyberbezpieczeństwu (Polityka Ochrony Cyberprzestrzeni), to nie

spełnia on wszystkich wymagań postawionych przez dyrektywę, brakuje m.in. jasno określonych celów, priorytetów, konkretnych działań, mechanizmów współpracy, określenia odpowiedzialności poszczególnych aktorów. Dlatego szerzej zostało omówione to w rozdziale 6. Ministerstwo Cyfryzacji zostało zlikwidowane 7.10.2020 r.

[496] Infrastruktura cyfrowa obejmuje punkty wymiany ruchu internetowego, dostawców usług systemu nazw domen, rejestrów nazw domen najwyższego poziomu.

[497] Szerzej: W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019, s. 30–50.

[498] Przepisy art. 17 i kolejnych ustawy formułują obowiązki dostawców usług cyfrowych, w rozdziale 11 natomiast uregulowano kwestie związane z nadzorem i kontrolą dostawców usług cyfrowych oraz podmiotów świadczących usługi w zakresie cyberbezpieczeństwa.

[499] Dz.U. z 2003 r. nr 3, poz. 25.

[500] Dz.Urz. UE L 350 z 30.12.2008.

[501] COM(2012) 10 final, 25.01.2012.

[502] Terminu tego polski ustawodawca nie dotrzymał, uchwalając ustawę o ochronie danych osobowych przetwarzanych w związku ze zwalczaniem i zapobieganiem przestępczości dopiero 14 grudnia 2018 r., czyniąc to z błędami i pominięciami.

[503] Dz.Urz. UE L 119, 4.5.2016, p. 89–131.

[504] Motyw 12 preambuły do dyrektywy 2016/680 w związku z motywem 19 preambuły do RODO *in fine*.

[505] Szerzej: A. Grzelak, *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości*. *Komentarz*, Warszawa 2019, s. 23.

[506] Podstawą funkcjonowania Agencji jest rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004 (Dz.Urz. UE L 165 z 18.06.2013).

[507] Szerzej: D. Adamski, *Europejskie prawo*, s. 48.

[508] https://www.europol.europa.eu/newsroom/news/expert-international-cybercrime-taskforce-launched-to-tackle-online-crime-0 (dostęp: 30.07.2020).

[509] P. Bryksy, *Wybrane zagadnienia polityki bezpieczeństwa wewnętrznego Unii Europejskiej. Szanse i zagrożenia dla Polski*, „Biuro Bezpieczeństwa Narodowego", Warszawa 2008, s.15–30.

[510] Zadania te mogą obejmować: a) gromadzenie, przechowywanie, przetwarzanie, analizę i wymianę informacji, przekazywanych zwłaszcza przez organy państw członkowskich, państw trzecich lub instytucji spoza Unii; b) koordynowanie, organizowanie i prowadzenie dochodzeń i działań operacyjnych, prowadzonych wspólnie z właściwymi organami państw

członkowskich lub w ramach wspólnych zespołów dochodzeniowych, w stosownych przypadkach w powiązaniu z Eurojustem.

[511] Zob.: www.euractiv.pl/eu2you/europol0 (dostęp: 11.10.2011).

[512] Ibidem.

[513] W. Czapliński, *Układy z Schengen jako przykład nowych form współpracy państw członkowskich UE*, w: M. Boguszewski (red.), *Polska policja na drodze do Unii Europejskiej*, Warszawa 2007, s. 97–98.

[514] A. Graś, *Porozumienie z Schengen – geneza i stan obecny*, w: P. Jaworski (red.), *Polska droga do Schengen. Opinie ekspertów*, Warszawa 2001, s. 19.

[515] System SIS I, będący poprzednikiem SIS II, został wprowadzony 25 marca 1995 r. i przedstawiony w rozdziale 1.1.2.

[516] Ideą tego projektu było utworzenie bazy danych wystarczająco stabilnej, by mogła obsługiwać w przyszłości „poszerzoną" Unię. Podstawę prawną powołania SIS II stanowią rozporządzenie Rady (WE) nr 2424/2001 z dnia 6 grudnia 2001 r. w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz decyzja Rady z dnia 6 grudnia 2001 r. w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji. W preambułach tych aktów podkreślono, że podstawę prawną powołania SIS II, niezbędną do tego, by umożliwić finansowanie rozwoju tego programu z budżetu UE, stanowią dwa odrębne instrumenty. Nie narusza to zasady, zgodnie z którą SIS II stanowi i powinien stanowić zintegrowany system. Na mocy rozporządzenia nr 2424/2001 i decyzji 2001/886/WSiSW System Informacyjny Schengen (SIS I) ustanowiony na podstawie tyt. IV KWS zostaje zastąpiony Systemem Informacyjnym Schengen II (SIS II), który umożliwia włączenie nowych państw członkowskich do tego systemu. Ponadto wspomniane akty prawne określają procedury tworzenia i rozwoju SIS II. Rozporządzenie nr 2424/2001 oraz decyzja 2001/886/WSiSW miały obowiązywać do 31 grudnia 2006 r. Okazało się jednak, że proces opracowywania SIS II będzie dłuższy, niż przewidywano. W związku z tym, w celu zapewnienia środków finansowych na rozwój SIS II po 31 grudnia 2006 r., powstała konieczność przedłużenia okresu obowiązywania omawianych aktów prawnych. W tym celu zostało wydane rozporządzenie Rady (WE) nr 1988/2006 z dnia 21 grudnia 2006 r., zmieniające wcześniejsze rozporządzenie nr 2424/2001 w sprawie rozwoju SIS II, oraz decyzja Rady z dnia 21 grudnia 2006 r., zmieniająca decyzję 2001/886/WSIW w sprawie SIS II.

[517] Europol, *Cybercrime: Improving international cooperation. GCCS2015 – Parallel session 4*, Discussion paper, www.enisa.europa.eu/activities/cert/events/files/ENISA_Europol_threat_assessment_2007_Dileone.pdf (dostęp: 8.07.2019).

[518] Dane z oficjalnej strony internetowej Europolu: https://www.europol.europa.eu/ec3 (dostęp: 17.07.2020).

[519] DZ.Urz. UE L 63 z 06.03.2002.

[520] Należy to interpretować zgodnie z art. 1 lit. a) jako śledztwa prowadzone w sprawach przestępstw, które wymagają dokonywania trudnych i wymagających

działań śledczych, mających powiązania z innymi państwami członkowskimi.

[521] Na jego czele stoi przewodniczący wybierany na trzyletnią kadencję (reelekcja jest dopuszczalna). Eurojust może powołać także dwóch wiceprzewodniczących, ale nie jest to wymóg konieczny. Wyniki wyborów są zatwierdzane przez Radę UE. Przewodniczący reprezentuje kolegium na zewnątrz, kieruje nim i nadzoruje zadania wykonywane przez dyrektora administracyjnego.

[522] Dyrektor administracyjny mianowany jest jednomyślnie przez Kolegium. Jego kadencja trwa pięć lat i podobnie jak w przypadku przewodniczącego jest odnawialna. Dyrektor stoi na czele Sekretariatu i odpowiada za bieżące zarządzanie Eurojustem oraz kierowanie personelem. Jednocześnie podlega nadzorowi przewodniczącego Kolegium.

[523] Jest mianowany przez Kolegium i znajduje się pod jego wyłącznym nadzorem. Do jego obowiązków należy zapewnienie, w sposób niezależny, legalności i zgodności z przepisami decyzji o przetwarzaniu danych osobowych; gwarantowanie przechowywania pisemnych rejestrów o przekazywaniu i odbiorze danych osobowych zgodnie z przepisami ustanowionymi w regulaminie organizacyjnym; zapewnienie, by osoby, których dotyczą dane, były na żądanie informowane o swoich prawach wynikających z niniejszej decyzji.

[524] Por.: H. Loiseau, L. Lemay, *Canada's Cyber Security Policy: a Tortuous Path Toward a Cyber Security Strategy*, w: D. Ventre (red.), *Cyber Conflict. Competing National Perspectives*, London 2012, s. 3–9.

[525] Nowością jest art. 68 TFUE, na podstawie którego RE określa strategiczne wytyczne planowania prawodawczego i operacyjnego w przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

[526] W sprawach dotyczących międzynarodowego wymiaru bezpieczeństwa wewnętrznego UE jedna z najważniejszych zmian polegała na wprowadzeniu udziału w posiedzeniach RE Wysokiego Przedstawiciela Unii ds. Zagranicznych i Polityki Bezpieczeństwa.

[527] Powołany na szczycie RE w Brukseli 25–26 marca 2004 r.

[528] D. Barrett, T. King, *Computer Networking Illuminated*, USA 2005, s. 73.

[529] J. Aycock, *Computer Viruses*, s. 239.

[530] M. Vink, *Limits of European Citizenship: European Integration and Domestic Immigration Policies*, „Constitutionalism Web-Papers" 2003, nr 4, s. 13–14.

[531] Art. 2 TUE.

[532] Komitet skupiał wyższych urzędników państwowych i Komisje zajmujące się współpracą sądową i policyjną. CATS wydawał również instrukcje Radzie Grupy Roboczej ds. Terroryzmu (WPT), która skupia państwowych i europejskich urzędników Komisji, zajmujących się zwalczaniem terroryzmu w obszarze III filaru.

[533] W dziedzinach objętych niniejszym tytułem państwa członkowskie wzajemnie się informują i konsultują ze sobą w ramach RE, mając na względzie

koordynację swoich działań. W tym celu ustanawiają współpracę między swymi właściwymi jednostkami administracyjnymi.

[534] Ibidem, s. 445.

[535] Por.: A. Grzelak, *Traktat formujący UE*, s. 86–97.

[536] Por.: A. Kańciak, *Unia Europejska*, s. 270–276.

[537] Szerzej: rozdział 6.

[538] W 1999 r., kiedy niewyłączne prawo inicjatywy KE zostało rozciągnięte na wszystkie obszary sprawiedliwości i spraw wewnętrznych, KE powołała Dyrekcję Generalną ds. Sprawiedliwości i Spraw Wewnętrznych. Początkowo rola Komisji była ograniczona ze względu zarówno na brak personelu, jak i ostrożną strategię polityczną w tej dziedzinie. Przewodniczący KE Romano Prodi przyjął bardziej aktywną rolę w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych niż jego poprzednik, wybierając wraz z komisarzem António Vitorino ambitny porządek obrad oraz szerokie wykorzystanie prawa inicjatywy Komisji, chociaż brak jej charakteru niewyłącznego i wymogu jednomyślności w dalszym ciągu ograniczały wagę polityczną KE w procesie podejmowania decyzji.

[539] Zob.: K. Lankosz (red.), *Traktat o Unii Europejskiej*, s. 63–75.

[540] „Decyzji" nie należy tu rozumieć zbyt formalnie, tj. w takim znaczeniu, w jakim to pojęcie występuje w art. 249 TWE. Wydaje się, że tak określona kompetencja stanowi ogólną podstawę wykonywania przez nie kompetencji prawodawczej.

[541] Zob.: I. Oleksiewicz, *Polityka antyterrorystyczna*, s. 172–200.

[542] J. Barcz (red.), *Traktat reformujący*, s. 146–147.

[543] Ten zapis najbardziej przypomina dotychczasowe art. 60 i art. 301 TWE, jednak w tym wypadku zmieniła się również procedura podejmowania decyzji. Jest również przedmiotem rozporządzenia Rady (WE) nr 2580/2001 z 27 grudnia 2001 r. w sprawie szczególnych środków restrykcyjnych skierowanych przeciwko niektórym osobom i podmiotom mającym na celu zwalczanie terroryzmu (Dz.Urz. WE L 344 z 28.12.2001).

[544] Oprócz zmiany nazwy z Komitetu Koordynacyjnego na Stały Komitet ds. Zapewnienia Wspierania i Wzmacniania Współpracy Operacyjnej Wewnątrz Unii zmodyfikowano przede wszystkim zakres zadań tego organu, zawężając je jedynie do czynności operacyjnych, a tym samym do współpracy w ramach policji.

[545] Wyrok z 3.06.2007 r. w sprawie C-303/05, Advocaten voor de Wereld v. Leden.

[546] Por.: wyrok SPI w sprawie T-229/02, PKK v. Rada.

[547] J. Brennan, *The Impact on Counterterrorism*, Harvard 2005, s. 69.

[548] Zmiana, na pierwszy rzut oka radykalna, okazuje się po bliższej analizie mniej przełomowa. Wprowadzenie przyjmowania dyrektyw kwalifikowaną większością głosów przez Radę zostało ograniczone do tych obszarów, które już zostały poddane harmonizacji w drodze decyzji ramowych, czyli aktów prawnych III filara. Ewentualna modyfikacja przepisów przyjętych lub uzgodnionych decyzji ramowych będzie się odbywała na podstawie TFUE i

doprowadzi do „przekształcenia” tych aktów w dyrektywy (ze wszystkimi konsekwencjami instytucjonalnymi i systemowymi tej zmiany). Szerzej: M. Szwarc-Kuczer, *Harmonizacja*, s. 10–17.

[549] I. Oleksiewicz, *Challenges of EU*, s. 34–35; B. Hoffman, *Is Europe Soft on Terrorism?*, „Foreign Policy” 1999, nr 115, s, 398.

[550] Szerzej: K. Kądziołka, *Ocena poziomu zagrożenia terroryzmem w krajach Unii Europejskiej z wykorzystaniem GTI*, „Ekonomia Międzynarodowa” 2018, nr 2, s. 94.

[551] O. Bures, H. Carrapico (red.), *Security Privatization. How Non-security-related Private Businesses Shape Security Governance,* Warszawa 2018, s. 57–58.

[552] Zadania te mogą obejmować: a) wszczynanie śledztwa karnego oraz występowanie z wnioskiem o wszczęcie ścigania prowadzonego przez właściwe organy państwowe, w szczególności dotyczącego przestępstw przeciwko interesom finansowym Unii; b) koordynację śledztw i ścigania, o których mowa w lit. a); c) wzmacnianie współpracy sądowej, w tym przez rozstrzyganie sporów o właściwość i ścisłą współpracę z Europejską Siecią Sądową.

[553] Szerzej: rozdział 6.

[554] Zadania te mogą obejmować: a) gromadzenie, przechowywanie, przetwarzanie, analizę i wymianę informacji przekazywanych zwłaszcza przez organy państw członkowskich, państw trzecich lub instytucji spoza UE; b) koordynowanie, organizowanie i prowadzenie dochodzeń i działań operacyjnych wspólnie z właściwymi organami państw członkowskich lub w ramach wspólnych zespołów dochodzeniowych, w stosownych przypadkach w powiązaniu z Eurojustem.

[555] Dz.Urz. UE C 53 z 3.03.2005.

[556] *Study on the Best Practices in Cooperation Between Authorities and Civil Society with a View to the Prevention and Response to Violent Radicalization*, Report by The Change Institute, London, July 2008, s. 26–39.

[557] P. Chalk, W. Rosenau, *Confronting the Enemy Within*, Santa Monica 2004, s. 1–5.

[558] Dz.Urz. WE C 316 z 27.11.1995.

[559] Dz.Urz. UE L 190 z 18.07.2002.

[560] Dz.Urz. UE L 162 z 20.06.2002.

[561] Decyzja Rady 2002/187/WSiSW z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością (Dz.Urz. UE L 63 z 06.03.2002).

[562] Communication from Commission to the Council and the European Parliament: Development of Schengen Information System II (COM(2001) 720, 18.12.2001).

[563] Dz.Urz. UE L 253 z 29.09.2005.

[564] Dz.Urz. UE L. 309 z 26.10.2005; A. Gruszczak, *Unia Europejska wobec przestępczości*, Kraków 2002, s. 159.

[565] Dz.Urz. WE L 281 z 23.11.1995.

[566] Dz.Urz. UE L 108 z 24.04.2002.
[567] Dz.Urz. UE L 201 z 31.07.2002.
[568] Dz.Urz. UE L 69 z 16.03.2005.
[569] Dz.Urz. UE C 198 z 12.08.2005.
[570] Dz.Urz. UE C 53 z 03.03.2005, s. 1.
[571] COM(2005) 184 final.
[572] Wynika to z komunikatu Komisji do Rady i Parlamentu Europejskiego z dnia 23 października 2007 r. w sprawie roli Eurojustu i Europejskiej Sieci Sądowej w zwalczaniu przestępczości zorganizowanej i terroryzmu.
[573] J. Ziller, *Le traité de Prüm Une vraie-fausse coopération renforcée dans l'Espace de sécurité de liberté et de justice*, „European University Institute Working Papers LAW" 2006, nr 32; A. Graś, *Konwencja z Prüm – pozytywne i negatywne konsekwencje*, „Biuletyn Analiz UKIE" 2006, nr 16, s. 6.
[574] Dok. 14469/4/05 Rev 4 Limite z 30.11.2005 r.
[575] Szerzej: F. Galloway, *Anti-Terrorism Resolutions: The Security Council's Threat to the UN System*, „Journal of Terrorism Research" 2011, vol. 2(3), s. 105 i n.
[576] COM(2006) 331 final; Dz.Urz. UE C 184 z 8.01.2006.
[577] COM(2006) 332, 333 i 346.
[578] I. Awan, *Paving the Way for Extremism: How Preventing the Symptoms Does Not Cure the Disease of Terrorism*, „Journal of Terrorism Research" 2011, vol. 2(3), s. 4–8.
[579] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, On Fighting Spam, Spyware and Malicious Software (COM(2006) 688 final, 15.11.2006).
[580] E. Shor, *Constructing a Global Counterterrorist Legislation Database: Dilemmas, Procedures, and Preliminary Analyses*, „Journal of Terrorism Research" 2011, vol. 2(3), s. 49 i n.
[581] COM(2007) 0267 final.
[582] Ibidem, s. 78.
[583] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Europejska agenda cyfrowa (COM(2010) 245 final, 16.5.2010).
[584] Zob.: Program sztokholmski – *Otwarta i bezpieczna Europa dla dobra i ochrony obywateli* (Dz.Urz. UE C 115 z 04.05.2010).
[585] M. Grajny, *The European Union Counterterrorism Policy Before and After the 9/11 Attacks: to Extend What Does EU Have an Integrated Policy Towards Terrorism*, Kraków 2008, s. 20.
[586] Na podstawie art. 19 TFUE należy stwierdzić, że Trybunał Sprawiedliwości UE jest właściwy w PWBiS w następujących sprawach: 1) w zakresie skarg wniesionych przez państwa członkowskie, instytucje lub osoby fizyczne lub prawne; 2) w trybie prejudycjalnym, na wniosek sądów państw członkowskich, w sprawie wykładni prawa Unii lub ważności aktów przyjętych przez instytucje;

3) w innych sprawach przewidzianych w traktatach. Oznacza to duży postęp w stosunku do obecnych rozwiązań, w których istnieją liczne ograniczenia w zakresie procedury prejudycjalnej. Trybunał nie będzie właściwy w zakresie kontroli ważności lub proporcjonalności działań policji lub innych organów ścigania w państwie członkowskim ani do orzekania w sprawie wykonania przez państwa członkowskie obowiązków dotyczących utrzymania porządku publicznego i ochrony bezpieczeństwa wewnętrznego. Warto zwrócić uwagę, że nastąpiło odejście od jednego ograniczenia istniejącego do tej pory w art. 68 ust. 2 TWE. Tymczasem ograniczenie przewidziane w TFUE będzie miało zastosowanie wyłącznie do spraw należących do współpracy sądowej w sprawach karnych i współpracy policyjnej.

[587] Szerzej: dok. DT/547811PL.doc 3/2 PE 350.051.

[588] R. Sawicki, *Z orzecznictwa Europejskiego Trybunału Sprawiedliwości. Orzeczenie Sądu I Instancji z dnia 11 lutego 2003 r. w połączonych sprawach C–187/01 i C–385/01*, „Prokuratura i Prawo" 2005, nr 2, s. 79–93.

[589] Decyzja Rady nr 2011/318/WPZiB z 31 marca 2011 r. w sprawie podpisania i zawarcia umowy ramowej między Stanami Zjednoczonymi Ameryki a Unią Europejską w sprawie udziału Stanów Zjednoczonych Ameryki w operacjach zarządzania kryzysowego prowadzonych przez Unię Europejską (Dz.Urz. UE L 143 z 31.05.2011).

[590] Por.: sprawa McCann i inni v. Wielka Brytania, wyrok z 27.09.1995 r.; sprawa Yasa v. Turcja, wyrok 2.09.1998 r.; Raport Europejskiej Komisji Praw Człowieka z 4 marca 1994 r. Por. też: B. Bolechów, *Terroryzm w świecie podwubiegunowym. Przewartościowania i kontynuacje*, Toruń 2002, s. 412.

[591] Ramy unijnej polityki obrony cybernetycznej (dok. 15585/14 z 18.11.2014, s. 12), https://www.consilium.europa.eu/media/37024/st14413-en18.pdf (dostęp: 12.02.2020).

[592] https://eeas.europa.eu/top_stories/pdf/eugs_pl_.pdf. (dostęp: 13.08.2020).

[593] Por.: M. Wróblewska-Łysik, *Europejska strategia*, s. 67–70.

[594] H. Wyligała, *Kształtowanie i monitorowanie strategii bezpieczeństwa wewnętrznego Unii Europejskiej*, „Rocznik Bezpieczeństwa Międzynarodowego" 2014, t. 8(1), s. 15.

[595] S. Biscop, *The EU*, s. 1–3.

[596] Zadania te mogą obejmować: a) gromadzenie, przechowywanie, przetwarzanie, analizę i wymianę informacji, przekazywanych zwłaszcza przez organy państw członkowskich, państw trzecich lub instytucji spoza Unii; b) koordynowanie, organizowanie i prowadzenie dochodzeń i działań operacyjnych, prowadzonych wspólnie z właściwymi organami państw członkowskich lub w ramach wspólnych zespołów dochodzeniowych, w stosownych przypadkach w powiązaniu z Eurojustem.

[597] Zob.: www.euractiv.pl/eu2you/europol0 (dostęp: 11.10.2020).

[598] Ibidem.

[599] W. Czapliński, *Układy z Schengen jako przykład nowych form współpracy państw członkowskich UE*, w: M. Boguszewski (red.), *Polska policja na drodze do Unii Europejskiej*, Warszawa 2007, s. 97–98.
[600] Dz.Urz. WE L 328 z 13.12.2001.
[601] 2001/886/WSiSW.
[602] Dz.Urz. UE L 27 z 02.02.2007.
[603] 2006/1007/WSiSW.
[604] Dz.Urz. UE L 381 z 28.12.2006.
[605] Dok. 14914/06 z 12.12.2006.
[606] Decyzja dotychczas nieopublikowana w Dz.Urz. UE, ale przyjęta 12 czerwca 2007 r., z wyjątkiem wersji w językach bułgarskim i rumuńskim.
[607] Dz.Urz. UE L 218 z 13.08.2008.
[608] Zgodnie z art. 1 „przestępstwa terrorystyczne" oznaczają przestępstwa w rozumieniu prawa państwowego, które odpowiadają przestępstwom określonym w art. 1–4 decyzji ramowej Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu lub są im równoważne.
[609] Dz.Urz. UE L 81 z 27.03.2009.
[610] Dz.Urz. UE L 205 z 07.08.2007.
[611] Por.: Uzasadnienie do Rady decyzją Rady powierzającą agencji ustanowionej na mocy rozporządzenia XX zadania dotyczące zarządzania operacyjnego systemami SIS II i VIS w zastosowaniu tyt. VI Traktatu UE (COM/2009/0294 końcowy – CNS 2009/0090).
[612] COM(2011) 907 final.
[613] A. Gruszczak, *Eurojust*, s. 76–86.
[614] ECRE, *The ECRE Tampere Dossier – A Compilation of Non and Inter-Governmental Observations on the Special Meeting of the European Council on the Establishment of an Area of Freedom, Security and Justice*, 15/16 October 1999, Tampere, Finland and a selection of Presentations made at the „ECRE EU Tampere Summit Parallel Meeting". Zob.: www.ecre.org (dostęp: 15.07.2020).
[615] Zob.: A. Gruszczak, *III filar Unii Europejskiej po Tampere: wnioski i perspektywy*, „Studia Europejskie" 2000, nr 3, s.10.
[616] Dz.Urz. UE L 63 z 05.03.2002.
[617] Dz.Urz. UE L 245 z 29.09.2003.
[618] Zob.: A. Gruszczak, *Eurojust*, s. 78.
[619] Decyzja Rady 2002/187/WSiSW z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością (Dz.Urz. UE L 63 z 5.03.2002).
[620] Por.: A. Gruszczak, *Eurojust*, s. 76–86.
[621] Zgodnie z art. 1 decyzji Rady Eurojust jest organem Unii Europejskiej, posiadającym osobowość prawną. Składa się z jednego przedstawiciela państwowego, oddelegowanego przez każde państwo członkowskie zgodnie ze swoim systemem prawnym, będącego prokuratorem, sędzią lub funkcjonariuszem policji o równoważnych kompetencjach. Każdemu

przedstawicielowi państwowemu mogą towarzyszyć zastępca i asystent. Gdy okaże się to niezbędne, przedstawicielowi państwowemu, za zgodą kolegium, może towarzyszyć kilka osób, a jedna z nich może zastąpić przedstawiciela państwowego. Kolegium składa się z przedstawicieli państwowych, każdy z nich ma jeden głos. Podejmuje decyzje większością dwóch trzecich głosów. Inne decyzje Kolegium podejmowane są zgodnie z regulaminem. Jest odpowiedzialne za organizację i działanie Eurojustu, wybiera przewodniczącego spośród przedstawicieli państwowych i może, jeśli uzna to za niezbędne, wybrać dwóch wiceprzewodniczących. Rezultaty wyborów przekazywane są Radzie do zatwierdzenia większością kwalifikowaną. Przewodniczący wykonuje swoje obowiązki na rzecz Kolegium i pod jego nadzorem, kieruje jego działaniami i nadzoruje zarządzanie nim. Kadencja przewodniczącego trwa trzy lata. Przewodniczący może być wybrany powtórnie na kolejną, ale tylko jedną kadencję. Kadencja wiceprzewodniczącego jest ustalana zgodnie z regulaminem.

[622] Podstawą funkcjonowania Agencji jest rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004 (Dz.Urz. UE L 165 z 18.06.2013).

[623] Dz.Urz. UE L 151 z 7.06.2019.

[624] IP/10/1535 i MEMO/10/598.

[625] Przyjęta jeszcze w 2006 r. *Strategia UE na rzecz bezpiecznego społeczeństwa informacyjnego w Europie* zwracała uwagę na problem cyberterroryzmu. Podkreślała, że ataki skierowane na prywatne lub rządowe systemy informatyczne w państwach członkowskich UE nadały mu nowy wymiar, jako potencjalnej nowej broni ekonomicznej, politycznej i wojskowej. Sugerowała, że w tym obszarze konieczne są dalsze prace w celu podniesienia poziomu świadomości i zacieśnienia współpracy unijnej. Szerzej: I. Oleksiewicz, *Polityka antyterrorystyczna*, s. 28.

[626] Patrz szerzej s. 171.

[627] Dz.Urz. UE L 201 z 31.07.2002.

[628] Dz.Urz. UE L 108 z 24.04.2002.

[629] Ibidem.

[630] Dz.Urz. UE L 69 z 16.03.2005.

[631] Dz.Urz. UE L 77 z 13.03.2004.

[632] Dz.Urz. WE L 281 z 23.11.1995.

[633] A. Suchorzewka, *Ochrona prawna*, s. 165.

[634] A. Wąsek, R. Zawłocki, *Komentarz do rozdziału XXXIII KK Przestępstwa przeciwko ochronie informacji*, s. 570–580; K. Lewandowski, *Przestępstwa przeciwko ochronie informacji w świetle Rozdziału XXXIII Kodeksu Karnego, orzecznictwa i doktryny*, „Wojskowy Przegląd Prawniczy" 2010, nr 3, s. 61 i n.

[635] *Dz.Urz. UE L 321 z 17.12.2018*.

[636] Agencja składa się z Zarządu, dyrektora naczelnego, który nią zarządza, oraz Stałej Grupy Udziałowców, składającej się z ekspertów reprezentujących

właściwych udziałowców z przemysłu technologii informacyjnych i łączności, grup konsumenckich oraz ekspertów akademickich w zakresie bezpieczeństwa sieci i informacji. W skład Zarządu wchodzi jeden przedstawiciel każdego z państw członkowskich, trzech przedstawicieli wyznaczonych przez Komisję oraz trzech przedstawicieli bez prawa głosowania zaproponowanych przez Komisję i wyznaczonych przez Radę. Zarząd określa ogólną orientację działania Agencji i zapewnia funkcjonowanie Agencji zgodnie z zasadami określonymi w rozporządzeniu. Zarząd gwarantuje również spójność pracy Agencji z działaniami państw członkowskich i Wspólnoty. T. Przesławski, *Cel w konstrukcji przestępstwa terrorystycznego*, „Prokuratura i Prawo" 2009, nr 5, s. 18.

[637] Zob. wyżej szczegóły.

[638] Dz.Urz. UE L 345 z 23.12.2008.

[639] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. UE L 218 z 14.08.2013).

[640] Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz.Urz. UE L 69 z 16.03.2005).

[641] A.M. Kruk, *Bezpieczeństwo transferu*, s. 345.

[642] A. Sakowicz, *Prawnokarne gwarancje prywatności,* Zakamycze 2006, s. 24. Por.: F. Radoniewicz, *Postanowienia decyzji*, s. 48.

[643] K. Gienas, *Systemy Digital Rights Management w świetle prawa autorskiego*, Warszawa 2008, s. 229.

[644] Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.Urz. UE L 335 z 17.12.2011).

[645] Dyrektywa Rady 2008/114/WE z grudnia 2008 r. w sprawie europejskiej infrastruktury krytycznej (Dz.Urz. UE L 345 z 23.12.2008).

[646] JOIN(2013) 1 final, 7.02.2013.

[647] Dz.Urz. UE UE L 194 z 19.07.2016, s. 1.

[648] Infrastruktura cyfrowa obejmuje punkty wymiany ruchu internetowego, dostawców usług systemu nazw domen, rejestrów nazw domen najwyższego poziomu.

[649] https://eeas.europa.eu/top_stories/pdf/eugs_pl_.pdf (dostęp: 13.08.2020).

[650] Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Strategia Bezpieczeństwa Cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (JOIN(2013) 1 final, 07.02.2013).

[651] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 194 z 19.07.2016).

[652] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE L 119 z 04.05.2016).

[653] Szerzej s. 101.

[654] Por.: Raport TE-SAT 2018–19, European Union Terrorism Situation and Trend Report 2019–2019 (dostęp: 30.06.2020).

[655] *Biała Księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania* (COM(2020) 65 final, 19.02.2020).

[656] Dz.Urz. UE L 194, s. 1.

[657] Postanowienie NSA z dnia 23.04.2020 r. w sprawie II GZ 97/20; wyrok WSA z 11.12.2019 r. w sprawie VI SA/Wa 1436/19.

[658] Szczegóły: rozdział 13 ustawy o krajowym systemie cyberbezpieczeństwa.

[659] Dawny art. 249 TUE dotyczący hierarchii źródeł prawa wtórnego.

[660] Por.: art. 4 pkt 2 dyrektywy NIS i art. 2 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa.

[661] Zob.: art. 9 ust. 1 pkt 3. Sektorowe zespoły zostały uregulowane w art. 44 ustawy o krajowym systemie cyberbezpieczeństwa.

[662] Szerzej na ten temat w 6.2.4.

[663] Istniejąca w ustawie o świadczeniu usług elektronicznych definicja systemu teleinformatycznego zawierała pierwszy i drugi element definicji, nie objęła jednak danych cyfrowych. W tym celu należało opracować definicję obejmującą również dane cyfrowe (por.: art. 2 pkt 14 ustawy).

[664] Art. 2 pkt 12 ustawy. Treść definicji ryzyka przyjętej na gruncie polskiej ustawy różni się od sposobu interpretacji tego pojęcia zawartego w art. 4 pkt 9 dyrektywy NIS. Zgodnie ze sformułowaną w art. 4 pkt 9 dyrektywy NIS definicją „ryzyko" oznacza „każdą dającą się racjonalnie określić okoliczność lub zdarzenie, które ma potencjalny niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych". Ustawodawca unijny powiązał zatem definicję ryzyka z pojęciem zagrożenia, a nawet dokonał utożsamienia tych pojęć.

[665] Art. 2 pkt 13 ustawy. Proces szacowania ryzyka polega na określeniu możliwości wystąpienia zagrożeń oraz potencjalnych strat. W związku z tym takie oszacowanie uwzględnia dwa kluczowe parametry: możliwość lub prawdopodobieństwo realizacji zagrożenia i jego skutki finansowe. Przy wyborze metody do tego służącej istnieją w zasadzie dwie możliwości:

– metoda ilościowej analizy ryzyka, w której operuje się miarą zdarzenia losowego – prawdopodobieństwem wyrażonym liczbą z przedziału [0,1],

– metoda jakościowa analizy ryzyka, gdzie operuje się opisowymi, arbitralnie dobieranymi miarami wyrażającymi możliwość zajścia zdarzenia. Szerzej: K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008, s. 83 i n.

[666] Art. 2 pkt 19 ustawy. Zarządzanie ryzykiem jest procesem permanentnym, ponieważ ryzyko ma charakter dynamiczny. Należy się liczyć z tym, że zachodzą

różne zdarzenia mogące mieć wpływ na jego poziom i rodzaj. Por.: A. Berlin, L. Brotherson, *Bezpieczeństwo defensywne*, s. 22; M. Cygan, M. Geilke, *Tworzenie systemu zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001:2014*, Wrocław 2015, s. 17.

[667] Art. 2 pkt 17 ustawy.

[668] Art. 2 pkt 11 ustawy. Na gruncie dyrektywy NIS występowanie zagrożenia jest tożsame z istnieniem ryzyka, podczas gdy ryzyko w ujęciu ustawodawcy polskiego oznacza wypadkową występującego potencjalnie zagrożenia i konsekwencji (szkody, krzywdy), jakie może ono wywołać. Ustawodawca polski wymaga zatem, by ustalenie istnienia ryzyka było wynikiem permanentnie realizowanego procesu polegającego na filtrowaniu cyberprzestrzeni w poszukiwaniu zdarzeń, a następnie dokonywaniu ich selekcji i oceny pod kątem skutków, jakie zdarzenia te mogą wywołać dla realizacji celów instytucji. Polski ustawodawca – jak należy sądzić – stoi na stanowisku, że zdarzenie samo w sobie nie stanowi ryzyka, ryzyko może bowiem powstawać dopiero wówczas, gdy przewidywalne konsekwencje zdarzeń będą stanowić naruszenie wartości istotnych dla instytucji.

[669] Do ustalenia zakresu pojęcia „usługi cyfrowe" niezbędne staje się uwzględnienie zarówno postanowień dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.Urz. UE L 178, s. 1), a także dyrektywy 98/34/WE Parlamentu Europejskiego i Rady z 22 czerwca 1998 r. ustanawiającej procedurę udzielania informacji w zakresie norm i przepisów technicznych (Dz.Urz. UE L 204, s. 37 ze zm.). Do celów zawartej w tej dyrektywie definicji wskazano, że użyte w niej sformułowanie „na odległość" oznacza usługę świadczoną bez równoczesnej obecności stron, natomiast wyrażenie „drogą elektroniczną" oznacza, że usługa jest przesyłana pierwotnie i otrzymywana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (włącznie z kompresją cyfrową) oraz przechowywania danych, i która jest całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, odbiornika radiowego, środków optycznych lub innych środków elektromagnetycznych. Przez świadczenie usługi „na indywidualne żądanie odbiorcy usług" należy natomiast rozumieć, że usługa świadczona jest przez przesyłanie danych na indywidualne żądanie (art. 2 pkt 2 dyrektywy technicznej).

[670] W rozdziale 6 zostały wskazane uprawnienia i wymagane kompetencje CSIRT, pełniące najważniejsze funkcje techniczne w systemie, obejmujące m.in. koordynację i obsługę poważnych, istotnych i krytycznych incydentów. Opisane zostały również sposoby realizacji współpracy z operatorami usług kluczowych, dostawcami usług cyfrowych, podmiotami publicznymi i sektorowymi zespołami cyberbezpieczeństwa. W przepisach szczegółowych zostały opisane także role o charakterze administracyjno-regulacyjnym, role oraz zależności, które powstają

między organem właściwym ds. cyberbezpieczeństwa a operatorem usługi kluczowej.

[671] Dz.U. z 2017 r. poz. 827 z późn. zm.

[672] Szerzej: *Shaping Europe's Digital Future*, Brussels, 9 June 2020, No. prev. doc.: 8098/1/20.

[673] Por.: Cyber Rapport ENISA 2019.

[674] Por.: *Challenges to effective EU cybersecurity policy 2019*, https://www.eca.europa.eu/ (dostęp: 30.07.2020).

[675] Dz.Urz. UE L 194 z 19.07.2016, s. 1.

[676] W. Krztoń, I. Oleksiewicz, *Bezpieczeństwo współczesnego społeczeństwa informacyjnego w cyberprzestrzeni*, Warszawa 2017, s. 30.

[677] Estonia jest stroną konwencji stambulskiej oraz konwencji lanzarotejskiej, podpisała także protokół dodatkowy do konwencji budapeszteńskiej, ale go nie ratyfikowała.

[678] Estoński kodeks karny z dnia 06.06.2001 r. (RT I 2001, 61, 364).

[679] Estoński kodeks postępowania karnego z dnia 12.02.2003 r. (RT I 2003, 27, 166).

[680] RT I 2004, 87, 593. Ustawa weszła w życie 1 stycznia 2005 r.

[681] Art. 1 ustawy.

[682] RT I 2007, 68, 421.

[683] W 2005 r. Estonia stała się pierwszym państwem na świecie, w którym wykorzystano Internet do głosowania w wyborach lokalnych.

[684] Estonia, jako pierwsze suwerenne państwo na świecie, stała się ofiarą zmasowanego cyberataku. W kwietniu i maju 2007 r. infrastruktura IT państwa została zaatakowana przez rosyjskich hakerów w odpowiedzi na przeniesienie, z centrum Tallina na cmentarz wojskowy, pomnika upamiętniającego żołnierzy Armii Czerwonej. Za pomocą DDoS670 zostały zaatakowane główne strony rządowe, a także instytucje komercyjne, banki, szkoły oraz dostawcy Internetu. Cyberatak odznaczał się znacznym stopniem zorganizowania. Dochodzenie pokazało, że jego źródło miało miejsce w Rosji, choć rosyjski rząd zaprzeczył jakimkolwiek związkom z incydentem. Fala ataków na infrastrukturę informatyczną nasilała się, blokując strony internetowe parlamentu, Ministerstwa Obrony i Sprawiedliwości, policji, banków i niezależnych gazet. Ataki ustały w maju, jednak unaoczniły, że tak małe państwo jak Estonia jest bezbronne wobec cyberterroryzmu lub innych form zmasowanej informatycznej napaści. Mimo że nie spowodowały znacznych szkód materialnych i realnego zagrożenia dla infrastruktury krytycznej, efekt psychologiczny był ogromny. Rząd estoński wyciągnął prawidłowe wnioski z omawianego incydentu, wprowadzając wiele nowych rozwiązań i uregulowań prawnych w różnych dziedzinach – bezpieczeństwa, bankowości, polityki oraz w innych sektorach. Można zaryzykować stwierdzenie, że atak stał się przyczynkiem do wkroczenia na bardziej zaawansowany technologicznie i prawnie etap estońskiej polityki cyberbezpieczeństwa.

[685] Szerzej: C. Czosseck, R. Ottis, A. Talihärm, *Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security*, „International Journal of Cyber Warfare and Terrorism" 2011, t. 1(1), s. 28.
[686] https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf (dostęp: 10.08.2020).
[687] https://www.itu.int/dms_pub/itu-d/opb/strategy/D-STR-GCI.01-2017-PDF-E.pdf (dostęp: 10.08.2020).
[688] Ibidem.
[689] *Cyber Security Strategy 2014–2020*, Ministry of Economic Affairs and Communication 2014, s. 5–7.
[690] RT I, 01.04.2016.
[691] RT I, 22.05.2018.
[692] Szerzej: M. Kamiński, *Ujednolicenie prawa w zakresie systemowych rozwiązań ochrony ludności i obrony cywilnej*, w: J. Gawęcka, J. Wojtycza (red.), *Współczesna obrona cywilna. Wyzwania, ryzyko, zagrożenia*, Piotrków Trybunalski 2018, s. 32––37.
[693] *Cyber Security Strategy 2019–2022*, Ministry of Economic Affairs and Communication 2019, s. 14–16.
[694] https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf (dostęp: 30.07.2020).
[695] Por.: M. Kamiński, *System cyberbezpieczeństwa Republiki Estonii. Czy warto wzorować się na estońskich rozwiązaniach prawno-organizacyjnych?*, w: W. Kitler, K. Chałbińska-Jentkiewicz, K. Badzimirowska-Masłowska (red.), *System bezpieczeństwa w cyberprzestrzeni RP*, Warszawa 2018, s. 127.
[696] https://www.bbn.gov.pl/ftp/SBN%20RP.pdf (dostęp: 30.06.2020).
[697] Zob.: R. Kupiecki, *Strategia Bezpieczeństwa Narodowego RP 2014 jako instrument polityki państwa. Uwarunkowania zewnętrzne i aspekty procesowe*, „Bezpieczeństwo Narodowe" 2015, nr 1, s. 12–15.
[698] Z. Nowakowski, H. Szafran, R. Szafran, *Strategia bezpieczeństwa narodowego Polski na tle strategii bezpieczeństwa wybranych państw*, Warszawa 2014, s. 15–20.
[699] https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf (dostęp: 20.07.2020).
[700] Szerzej: S. Koziej, *Braki Strategii Bezpieczeństwa Narodowego 2020: bez koncepcji operacyjnej i priorytetów operacyjnych*, https://pulaski.pl/pulaski-policy-paper-s-koziej-braki-strategii-bezpieczenstwa-narodowego-2020-bez-koncepcji-operacyjnej-i-priorytetow-preparacyjnych/ (dostęp 25.07.2020).
[701] *Strategia rozwoju bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022* z 9 kwietnia 2013 r., s. 32.
[702] http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html (dostęp: 15.07.2020).

[703] Szerzej: M. Adamczuk, K. Liedel, *Doktryna cyberbezpieczeństwa RP*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 286.
[704] J. Michniak, *Bezpieczeństwo teleinformatyczne w zarządzaniu kryzysowym*, Warszawa 2004, s. 37.
[705] V. Pitts, *Cyber Crimes*, s. 163.
[706] E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011, s. 11; P. Mickiewicz, *System bezpieczeństwa narodowego w rozwiązaniach systemowych wybranych państw*, Warszawa 2018, s. 77.
[707] https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf (dostęp: 30.06.2020).
[708] A. Golonka, *Cyberprzestępczość – międzynarodowe standardy zwalczania zjawiska a polskie regulacje prawne*, „Studia Prawnicze. Rozprawy i Materiały" 2016, nr 1(18).
[709] C. McLeish, *Recasting the Threat of Chemical Terrorism in the EU: The Issue of Returnees from the Syrian Conflict*, „European Journal of Risk Regulation" 2017, nr 8(4).
[710] E. Nanopoulos, *The Fight against Terrorism, Fundamental Rights and the EU Courts: The Unsolved Conundrum*, „Cambridge Yearbook of European Legal Studies" 2012, nr 14.
[711] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, s. 3.
[712] Uchwała nr 52/2017 Rady Ministrów w sprawie Rządowego Programu Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2017–2022 (niepublikowana w M.P.).
[713] Por.: *Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011–2016*, http://bip.msw.gov.pl/bip/programy/19057,dok.html (dostęp: 02.07.2020).
[714] Dz.U. z 2018 r. poz. 762.
[715] Dz.U. z 2015 r. poz. 2281.
[716] M.P. z 2019 r. poz. 1037.
[717] https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/ (dostęp: 29.06.2020).
[718] M.P. z 2019 r., poz. 1037.
[719] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie). Akt o cyberbezpieczeństwie (*Cybersecurity Act* – CA) to druga po dyrektywie NIS ogólnoeuropejska regulacja w dziedzinie cyberbezpieczeństwa. CA składa się z dwóch części:
– nowy permanentny mandat dla ENISA, której nazwa została zmieniona z Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji na Agencję UE ds. Cyberbezpieczeństwa. Jej rola została znacznie wzmocniona nie tylko przez permanentny mandat, lecz także przez wiele nowych obowiązków związanych z wejściem w życie Dyrektywy NIS oraz europejskich ram certyfikacji;

– rozporządzenie tworzące europejskie ramy certyfikacji cyberbezpieczeństwa dla produktów i usług ICT. To bardzo istotna regulacja, która znacznie zmieni funkcjonujący obecnie model certyfikacji, zdominowany przez SOG-IS (*Senior Official Group Information Security Systems*). Akt o cyberbezpieczeństwie wszedł w życie 27 czerwca 2019 r.

[720] Dz.Urz. UE L 194 z 06.07.2016.

[721] Dyrektywa określa, jakim obowiązkom z zakresu bezpieczeństwa będą podlegać operatorzy usług kluczowych (sektory krytyczne, takie jak energetyka, transport, opieka zdrowotna i finanse) oraz dostawcy usług cyfrowych (internetowe platformy handlowe, wyszukiwarki, usługi przetwarzania w chmurze). Dyrektywa wymaga, aby każde państwo UE posiadało strategię bezpieczeństwa sieci i informacji. Choć Polska posiada bardzo ważny dokument poświęcony cyberbezpieczeństwu (*Polityka Ochrony Cyberprzestrzeni*), pod względem jakości nie spełnia on wymagań postawionych przez dyrektywę. Brakuje m.in. jasno określonych celów, priorytetów, konkretnych działań, mechanizmów współpracy, określenia odpowiedzialności poszczególnych aktorów. Dlatego właśnie Ministerstwo Cyfryzacji opracowało *Strategią cyberbezpieczeństwa RP*.

[722] O ile problem ten jest prawnie uregulowany w Europie czy w Ameryce Płn., o tyle np. Afryka czy Australia dopiero zaczynają stawiać pierwsze kroki regulacyjne w tym zakresie.

[723] S.P. Huntington, *Zderzenie cywilizacji*, s. 27.

[724] Szerzej: NATO StratCom COE, *2007 cyber attacks on Estonia*, s. 5–8.

[725] Por.: S. Malešević, *Terrorism*, s. 346.

[726] A. Jaroszewska, *Wybrane aspekty cyberprzestępczości w cyberprzestrzeni. Studium prawno-karne i kryminologiczne*, Olsztyn 2017.

[727] G. de Kerchove, C. Horn., *Counter-Terrorism*, s. 270–275.

[728] M. Albahar, *Cyber Attacks*, s. 993–1006.

[729] Por.: R. Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, „Cooperative Cyber Defence Centre of Excellence", Tallinn 2008, s. 30–32; NATO StratCom COE, *2007 cyber attacks on Estonia*, s. 8–10.

[730] Szerzej: K. Michalski, I. Oleksiewicz, E. Sienkiewicz, *Bezpieczeństwo online*, s. 154–156.

[731] Por.: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku*, http://cert.gov.pl (dostęp: 27.05.2019).

[732] Ibidem.

[733] Dz.U. z 1997 r. Nr 90, poz. 557 z późn. zm.

[734] A. Marek, *Kodeks karny. Komentarz*, Warszawa 2010, s. 532.

[735] Pojęcie „hakerstwo" oznacza włamanie do systemu informatycznego i sieci komputerowej z pokonaniem ustanowionych zabezpieczeń, mających chronić dostęp do przechowywanych i przetwarzanych informacji.

[736] Uchwała SN z 22.01.2003 r., I KZP 43/02, OSNKW 2003, nr 1, poz. 5.

[737] A. Wąsek, R. Zawłocki (red.), *Komentarz*, s. 513. Por. też: P. Kardas, *Prawnokarna ochrona informacji z perspektywy przestępstw komputerowych*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, t. 4(1), s. 67 i n.

[738] A. Suchorzewska, *Ochrona prawna*, s. 36–37.

[739] R. Zawłocki, *Przestępstwa przeciwko przedsiębiorcom. Komentarz*, Warszawa 2003, s. 20.

[740] Konwencja została przyjęta w Budapeszcie 23 listopada 2001 r. Jej stronami jest 41 państw. Sejm uchwalił ustawę ratyfikującą 12 września 2014 r. Prezydent podpisał ją 28 października 2014 r. Ustawa weszła w życie 19 listopada 2014 r. (Dz.U. z 2014 r. poz. 1514).

[741] J. Giezek (red.), *Kodeks karny. Komentarz*, Warszawa 2007, s. 242.

[742] Por.: M. Janowski, *Przestępstwo tzw. oszustwa komputerowego*, „Prokuratura i Prawo" 2011, nr 10, s. 52–53.

[743] Zob.: M. Dąbrowska-Kardas, P. Kardas, *Przestępstwa przeciwko mieniu*, w: *Nowa Kodyfikacja Karna. Kodeks karny*, z. 21, Warszawa 1998, s. 216.

[744] O. Górniok, *Kodeks karny. Komentarz*, Gdańsk 2008, s. 364. Zob. też: R. Góral, *Kodeks karny. Komentarz praktyczny*, Warszawa 2007, s. 497.

[745] A. Zoll (red.), *Kodeks karny – część szczególna. Komentarz*, t. II, Warszawa 2012, s. 1479 i n.

[746] Zob.: B. Fischer, *Przestępstwa komputerowe i ochrona informacji*, Kraków 2000, s. 146.

[747] Szerzej: E. Pływaczewski, *Kodeks karny. Komentarz*, Warszawa 2010, s. 1034.

[748] Por.: R. Korczyński, R. Koszut, *„Oszustwo" komputerowe*, „Prokuratura i Prawo" 2002, nr 2, s. 32.

[749] Tzw. oszustwo telekomunikacyjne polega na narażeniu abonenta bądź operatora telekomunikacyjnego na szkodę majątkową w wyniku włączenia się do urządzenia telekomunikacyjnego i uruchomienia impulsów telefonicznych na ich koszt.

[750] A. Marek, *Kodeks karny*, s. 527.

[751] A. Adamski, *Cyberprzestępczość – rozwój*, s. 167.

[752] K. Gienas, *Systemy digital*, s. 259.

[753] Dz.U. z 2011 r. nr 72, poz. 381.

[754] Przed wejściem w życie przepisów art. 190a k.k. na gruncie polskiego prawa karnego do walki z nękaniem można było stosować niektóre z przepisów *Kodeksu karnego* lub *Kodeksu wykroczeń*, np. art. 107 k.w. (złośliwe niepokojenie); art. 207 k.k. (znęcanie się); art. 190 k.k. (groźba karalna); art. 191 k.k. (zmuszanie); art. 193 k.k. (naruszenie miru domowego); art. 202 § 3 k.k. (rozpowszechnianie tzw. twardej pornografii) Szerzej: M. Mozgawa, w: J. Warylewski (red.), *Przestępstwa przeciwko dobrom indywidualnym*, t. 10, Seria: *System Prawa Karnego*, Warszawa 2016, s. 454.

[755] M. Szymczak (red.), *Słownik języka polskiego*, t. II, Warszawa 1984, s. 317.

[756] M. Mozgawa, w: J. Warylewski (red.), *Przestępstwa*, s. 460.

[757] W wyroku SN z 5.01.2001 r. (V KKN 504/00, OSNKW 2001/7–8, poz. 57) stwierdzono, że uporczywość jest antynomią jednorazowego czy nawet kilkakrotnego zachowania sprawcy. Widać zatem, jak judykatura podchodziła do zagadnienia uporczywości (na gruncie art. 209 k.k. przed nowelizacją z 23.03.2017) i należy sądzić, że takie samo podejście będzie prezentowane na gruncie art. 190a k.k. Widoczne jest pewne podobieństwo między znęcaniem się a nękaniem. Warto jednak zwrócić uwagę, że w konstrukcji art. 207 użyto określenia „Kto znęca się…", a nie „Kto uporczywie znęca się…" i taka sama koncepcja powinna być przyjęta w art. 190a. Można zaryzykować pogląd, że przez użycie znamienia uporczywości *de facto* ustawodawca w istotny sposób zawęził prawnokarną ochronę pokrzywdzonego. Por.: M. Mozgawa, w: J. Warylewski (red.), *Przestępstwa*, s. 441).

[758] M. Mozgawa, w: J. Warylewski (red.), *Przestępstwa*, s. 464.

[759] M. Mozgawa, M. Budyn-Kulik, *Prawnokarne i kryminologiczne aspekty zjawiska nękania*, Warszawa 2012, s. 28; Por. też: K. Nazar*, Glosa do postanowienia Sądu Najwyższego z dnia 12 grudnia 2013 r.*, „Prawo w Działaniu Sprawy Karne" 2016, nr 26, s. 241 i n.

[760] Por. też: wyrok NSA z 18.11.2009 r., I OSK 667/09.

[761] A. Lach, *Kradzież tożsamości*, „Państwo i Prawo" 2012, nr 3, s. 34; J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych*, s. 374.

[762] Dz.U. z 2018 r. poz. 1000.

[763] A. Zoll (red.), *Kodeks karny*, s. 607.

[764] Ibidem, s. 567.

[765] A. Lach, *Kradzież tożsamości*, s. 38.

[766] Szerzej: M. Mozgawa, w: J. Warylewski (red.). *Przestępstwa*, s. 475–476.

[767] Zob. wyżej przyp. 64.

[768] Dz.U. z 1997 r. Nr 90, poz. 557 z późn. zm.

[769] M. Janowski, *Przestępstwo*, s. 52–53.

[770] Por.: O. Górniok, *Kodeks karny*, s. 408; E. Pływaczewski, *Kodeks karny*, s. 1034.

[771] Oszustwo komputerowe oznacza w tym przypadku działanie sprawcy w celu osiągnięcia korzyści majątkowej.

[772] Szkodnictwo komputerowe wiąże się z zamiarem wyrządzenia szkody majątkowej.

[773] A. Marek, *Kodeks karny. Komentarz*, Warszawa 2010, s. 527. Zob. też: R. Góral, *Kodeks karny*, s. 497.

[774] Por.: J. Giezek (red.), *Kodeks karny. Komentarz*, Warszawa 2007, s. 242.

[775] Por.: A. Suchorzewska, *Ochrona prawna*, s. 241–244.

[776] Przestępstwo to polega na narażeniu abonenta bądź operatora telekomunikacyjnego na szkodę majątkową w wyniku włączenia się do urządzenia telekomunikacyjnego i uruchomienia impulsów telefonicznych na ich koszt.

[777] Osoby korzystające z usług telekomunikacyjnych na cudzy rachunek.

[778] Por.: I. Oleksiewicz, K. Stachurska-Szczesiak, *Oszustwo komputerowe a polityka bezpieczeństwa informacyjnego Polski*, w: Bogdalski P. i in. (red.), *Współczesne zagrożenia cyberterrorystyczne i bioterrorystyczne a bezpieczeństwo narodowe Polski*, Warszawa–Dęblin 2015.

[779] Dz.U. z 1997 r. Nr 78, poz 483 z późn. zm.

[780] Dz.U. z 2019 r. poz. 945 z późn zm.

[781] Dz.U. z 2019 r. poz. 1398 z późn. zm.

[782] S. Kowalkowski (red.), *Niemilitarne zagrożenia*, s. 53; M. Czyżak, *Cyberprzestępczość*, s. 665–673.

[783] Zarządzenie nr 10/MON Ministra Obrony Narodowej z dnia 29 kwietnia 2013 r. w sprawie utworzenia i nadania statutu państwowej jednostce budżetowej – Narodowe Centrum Kryptologii, Warszawa, 29 kwietnia 2013, s. 3 (Dz.Urz. MON z 2013 r. poz. 121).

[784] Jest to instytucja powstała na mocy ustawy z dnia 24 maja 2002 r. (Dz.U. z 2002 r. nr 93, poz. 829).

[785] Została utworzona ustawą z dnia 6 kwietnia 1990 r. (Dz.U. 1990 r. nr 30, poz. 179 z późn. zm.). Ustawa nie zawiera wprost zapisu mówiącego o zwalczeniu terroryzmu, ale policja czyni to na podstawie przepisów zawartych w *Kodeksie karnym*, np. 163, 165–168 k.k.

[786] Dz.U. z 2017 r. poz. 1920 i 2405 oraz z 2018 r. poz. 138, 650, 723 i 730.

[787] *Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami. Analiza sytuacji i rekomendacje działań*, „Cyfrowa Polska", Warszawa 2019. Por.: H. Cornwall, *Datatheft*.

[788] Por.: D. Barrett, T. King, *Computer*.

[789] M. Młotek, M. Siedlarz, *Rządowy Zespół Reagowania na Incydenty Komputerowe. CERT.GOV.PL,* „Przegląd Bezpieczeństwa Wewnętrznego" 2011, nr 4, s. 161.

[790] Por.: I. Oleksiewicz, *Zarys polityki*, s. 123–130.

[791] Komendant CBŚP jest powoływany i odwoływany przez Ministra Spraw Wewnętrznych na wniosek Komendanta Głównego Policji. Zastępców nowej jednostki będzie powoływał szef policji na wniosek komendanta Centralnego Biura Śledczego Policji. Centralne Biuro Śledcze Policji będzie funkcjonowało na wzór komend wojewódzkich oraz komendy stołecznej. Komendant CBŚP będzie posiadał uprawnienia m.in. w zakresie czynności operacyjno-rozpoznawczych dotyczących kontroli operacyjnej oraz odnoszących się do czynności kontrolowanego przejęcia przedmiotów pochodzących z przestępstwa, czynności kontrolowanego wręczenia korzyści majątkowej, przedłużania tych czynności i ich kontynuowania oraz przekazywania prokuratorowi zgromadzonych materiałów. Komendant nowej jednostki będzie mógł także występować z wnioskami o udostępnienie danych telekomunikacyjnych oraz danych osób korzystających z usług pocztowych. Szerzej: E.M Guzik-Makaruk, *Regulacje prawne przewidziane w prawie policyjnym*,

w: E.W. Pływaczewski (red.), *Przestępczość zorganizowana*, Warszawa 2011, s. 281 i n.

[792] Ustawa weszła w życie 9 października 2014 r. (Dz.U. z 2014 r. poz. 1199).

[793] T. Płusa, *Aktualne trendy w bioterroryzmie i w obronie przed nim*, w: Bogdalski P. i in. (red.), *Współczesne zagrożenia cyberterrorystyczne i bioterrorystyczne a bezpieczeństwo narodowe Polski*, Warszawa–Dęblin 2015, s. 407.

[794] Została powołana na mocy ustawy z dnia 24 maja 2002 r. o utworzeniu ABW i AW (Dz.U. z 2010 r. nr 29, poz. 154).

[795] Swoje uprawnienia uzyskał dzięki ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 16 listopada 2000 r. (Dz.U. z 2003 r. nr 153, poz. 1505 z późn. zm.). GIIF ma z kolei za zadanie zapobiegać potencjalnemu przestępstwu finansowania terroryzmu określonego w art. 165a k.k. Na podstawie przepisów ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu uzyskuje, gromadzi, przetwarza i analizuje informacje, które mogą mieć związek m.in. z finansowaniem terroryzmu.

[796] Została powołana na podstawie ustawy z 12 października 1990 r. (Dz.U. z 2005 r. nr 234, poz. 1997 ze zm.). Do jej zadań należy zapobieganie nielegalnym migracjom osób podejrzanych o działalność terrorystyczną, przechwytywanie nielegalnych transportów zawierających szkodliwe substancje chemiczne, materiały jądrowe i wybuchowe.

[797] Art. 4 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2017 r. nr 0, poz. 1049).

[798] http://www.msz.gov.pl (dostęp: 30.06.2020).

[799] Jest instytucją międzynarodową zaangażowaną w walkę z finansowaniem terroryzmu powstałą w 1995 r. w Brukseli jako organizacja nieformalna, skupiająca przedstawicieli jednostek analityki finansowej, początkowo z państw UE oraz z USA. W 2007 r. podjęto decyzję o przekształceniu tej grupy skupiającej jednostki analityki finansowej ze 105 państw w formalną organizację międzynarodową. Szerzej: http://www.antyterroryzm.gov.pl/CAT/antyterroryzm/wspolpraca-zagraniczna/walka-z finansowaniem/565,Walka-z-finansowaniem-terroryzmu.html (dostęp: 30.06.2020).

[800] Dz.U. z 2012 r. poz. 461 z późn. zm.

[801] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247).

[802] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. z 2018 r. poz. 452, 650 i 730).

[803] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2017 r. poz. 209 i 1566).

[804] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138 i 650).

[805] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. z 2017 r. poz. 1876, 2361 i 2491 oraz z 2018 r. poz. 62, 106, 138, 650, 685 i 723).
[806] Dz.U. z 2017 r. poz. 2067 i 2405 oraz z 2018 r. poz. 106, 138, 416, 650 i 730.
[807] Dz.U. z 2017 r. poz. 209 i 1566.
[808] Dz.U. z 2017 r. poz. 2204 oraz z 2018 r. poz. 20, 305 i 663.
[809] Dz.U. z 2016 r. poz. 922 oraz z 2018 r. poz. 138 i 723.
[810] Dz.U. z 2017 r. poz. 2077 oraz z 2018 r. poz. 62.
[811] Dz.U. z 2018 r. poz. 395, 398 i 650.
[812] Dz.U. z 2016 r. poz. 1764 oraz z 2017 r. poz. 933.
[813] Dz.U. z 2017 r. poz. 2159 i 2203.
[814] Dz.U. z 2017 r. poz. 1845 oraz z 2018 r. poz. 697.
[815] Dz.U. z 2018 r. poz. 217, 357, 398 i 650.
[816] Dz.U. z 2016 r. poz. 1579 oraz z 2018 r. poz. 650.
[817] Dz.U. z 2017 r. poz. 1219 oraz z 2018 r. poz. 650.
[818] Dz.U. z 2016 r. poz. 1068, z 2017 r. poz. 60 oraz z 2018 r. poz. 650.
[819] Dz.U. z 2018 r. poz. 419.
[820] Szerzej kwestie te zostały opisane w rozdziale 3.3, a ustawa reguluje je w rozdziałach 6, 8, 9, 10 i 13.
[821] Ze względu na różnice w krajowych strukturach zarządzania państwa członkowskie mogą wyznaczać więcej niż jeden właściwy organ państwowy odpowiedzialny za wykonywanie zadań związanych z cyberbezpieczeństwem operatorów usług kluczowych i dostawców usług cyfrowych.
[822] Zadaniem Pojedynczego Punktu Kontaktowego jest wzmacnianie współpracy między państwami członkowskimi. PPK będzie gromadził informacje o incydentach w skali kraju i przez kontakt ze swoimi odpowiednikami z zagranicy wzmacniał wymianę informacji o znaczących transnarodowych incydentach.
[823] Przepisy art. 17 i kolejnych ustawy formułują obowiązki dostawców usług cyfrowych, w rozdziale 11 natomiast uregulowano kwestie związane z nadzorem i kontrolą dostawców usług cyfrowych oraz podmiotów świadczących usługi w zakresie cyberbezpieczeństwa.
[824] Ustawa umiejscowiła je odpowiednio przy Agencji Bezpieczeństwa Wewnętrznego, Ministrze Obrony Narodowej oraz Naukowej i Akademickiej Sieci Komputerowej. Zespoły CSIRT są opisane w art. 26 ustawy.
[825] Postanowienie NSA z dnia 23 kwietnia 2020 r. w sprawie II GZ 97/20; wyrok WSA z 11.12.2019 r. w sprawie VI SA/Wa 1436/19.
[826] Szczegóły: rozdział 13 ustawy o krajowym systemie cyberbezpieczeństwa.
[827] Dawny art. 249 TUE dotyczący hierarchii źródeł prawa wtórnego.
[828] Por.: art. 4 pkt 2 dyrektywy NIS i art. 2 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa.
[829] Zob.: art. 9 ust. 1 pkt 3. Sektorowe zespoły zostały uregulowane w art. 44 ustawy o krajowym systemie cyberbezpieczeństwa.
[830] O tym, co jest, a co nie jest incydentem poważnym, jest mowa w rozporządzeniu Rady Ministrów z 31 października 2018 r. w sprawie progów

uznania incydentu za poważny (Dz.U. z 2018 r. poz. 2180). Incydenty poważne dotyczą tylko usług kluczowych. Rozporządzenie wskazuje sektor, podsektor, nazwę zdarzenia oraz progi istotności, które muszą być przekroczone, aby incydent można było uznać za poważny. Brak dokonania zgłoszenia incydentu poważnego grozi nałożeniem administracyjnej kary finansowej.

[831] Incydent istotny (art. 2 pkt 8 ustawy – incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji UE 2018/151 z 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady UE 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych oraz parametrów służących do określenia, czy incydent ma istotny wpływ – Dz.Urz. UE L 26 z 31.01.2018, s. 48) to incydent podlegający obowiązkowi zgłaszania przez dostawców usług cyfrowych. Progi incydentu istotnego są określone w rozporządzeniu wykonawczym 2018/151.

[832] Incydent w podmiocie publicznym (art. 2 pkt 9 ustawy – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15) to incydent podlegający obowiązkowi zgłaszania przez podmioty publiczne. Komentowana ustawa (ani żadna inna ustawa) nie definiuje wprost, czym są zadania publiczne. Konieczne jest tutaj sięgnięcie do interpretacji z innych dziedzin.

[833] Incydent krytyczny (art. 2 pkt 6 ustawy – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GO).

[834] Dyrektywa NIS tworzy w art. 4 pkt 7 definicję dotyczącą „incydentu", później rozróżniając, że incydenty mogą dotyczyć różnego stopnia zagrożenia i różnych podmiotów. Dla czytelności obowiązków wybrano model definicyjny, w którym wskazano różne rodzaje incydentów wprost w słowniczku. W ten sposób pojawiły się następujące definicje:

– incydent,
– incydent poważny,
– incydent istotny,
– incydent w podmiocie publicznym,
– incydent krytyczny.

[835] Taka sama definicja występuje w art. 2 pkt 3 ustawy o świadczeniu usług drogą elektroniczną.

[836] Por.: art. 2 pkt 10 ustawy o krajowym systemie cyberbezpieczeństwa i art. 12 dyrektywy NIS.

[837] Por.: art. 2 pkt 18 ustawy o krajowym systemie cyberbezpieczeństwa i art. 4 pkt 8 dyrektywy NIS.
[838] Art. 2 pkt 11 ustawy o krajowym systemie cyberbezpieczeństwa.
[839] Art. 2 pkt 17 ustawy o krajowym systemie cyberbezpieczeństwa.
[840] a) Podsektor energii elektrycznej: zgodnie z przepisami dyrektywy 2016/1148 załącznik do ustawy obejmuje przedsiębiorstwa energetyczne, operatorów systemu dystrybucyjnego, operatorów systemu przesyłowego. Ustawa odwołuje się tutaj do regulacji zawartych w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, gdzie zdefiniowano przedsiębiorstwo energetyczne jako podmiot prowadzący działalność gospodarczą w zakresie wytwarzania, przetwarzania, magazynowania, przesyłania, dystrybucji energii lub obrotu nimi albo przesyłania dwutlenku węgla oraz regulacji w art. 3 pkt 24 i 25, gdzie odpowiednio uregulowano operatora systemu przesyłowego i operatora systemu dystrybucyjnego.

b) Podsektor ropy naftowej: regulacją będą objęci operatorzy ropociągów oraz operatorzy instalacji służących do produkcji, rafinacji, przetwarzania, magazynowania i przesyłu ropy naftowej. Podobnie jak w przypadku energii elektrycznej ustawa odwołuje się do definicji przedsiębiorstwa energetycznego z art. 3 pkt 12 ustawy.

c) Podsektor gazu: regulacją mogą zostać objęte przedsiębiorstwa dostarczające gaz, operatorzy systemu przesyłowego, operatorzy systemu dystrybucyjnego, operatorzy systemu magazynowania, operatorzy systemu LNG, przedsiębiorstwa gazowe, operatorzy instalacji służących do rafinacji i przetwarzania gazu ziemnego. W polskim systemie prawnym regulacje dotyczące omawianego sektora znajdują się w wymienionej wcześniej ustawie prawo energetyczne. Załącznik odwołuje się do art. 3 pkt 12 i art. 3 pkt 24–27 ustawy – Prawo energetyczne.

d) Podsektor wydobywania kopalin: podsektor nie jest zdefiniowany w dyrektywie 2016/1148, a jego obecność jest wymagana dla zachowania ciągłości łańcucha dostaw dla sektora energii. Podsektor ten obejmuje podmioty prowadzące działalność gospodarczą w zakresie wydobywania ropy naftowej, węgla kamiennego, węgla brunatnego i pozostałych kopalin na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.

e) Podsektor ciepło: podsektor nie jest zdefiniowany w dyrektywie 2016/1148. Podsektor ten obejmuje przedsiębiorstwa energetyczne posiadające koncesje na wykonywanie działalności gospodarczej w zakresie wytwarzania, obrotu, przesyłu, dystrybucji ciepłem, zdefiniowane w ustawie – Prawo energetyczne.

f) Podsektor dostaw i usług dla sektora energii i jednostki organizacyjne podległe ministrowi właściwemu do spraw energii lub przez niego nadzorowane oraz podmioty prowadzące działalność gospodarczą w zakresie dostaw systemów, maszyn, urządzeń, materiałów, surowców oraz świadczenia usług na rzecz sektora energii.

g) Katalog podmiotów ma obejmować ponadto podmioty prowadzące działalność gospodarczą w zakresie świadczenia usług systemowych, jakościowych i zarządzania infrastrukturą energetyczną, przedsiębiorstwa energetyczne prowadzące działalność gospodarczą w zakresie przetwarzania albo magazynowania energii elektrycznej, prowadzące działalność gospodarczą w zakresie przeładunku i obrotu paliwami ciekłymi, w tym ropy naftowej oraz podmiotów prowadzących działalność w zakresie wytwarzania paliw syntetycznych.

h) Podsektor transportu lotniczego: załącznik do ustawy wskazuje na przewoźników lotniczych, zarządzających lotniskiem, jednostki obsługujące urządzenia pomocnicze znajdujące się w portach lotniczych, operatorów zarządzających ruchem lotniczym zapewniających służbę kontroli ruchu lotniczego (ATC). Załącznik odwołuje się zatem do rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego, a także odpowiednich przepisów ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.

i) Podsektor transportu kolejowego: zgodnie z wytycznymi dyrektywy 2016/1148 regulacja ma obejmować zarządców infrastruktury, przedsiębiorstwa kolejowe i operatorów obiektów infrastruktury usługowej. W polskim systemie prawnym regulowany jest sektor ten ustawą o transporcie kolejowym. Wszystkie wymienione pojęcia zostały zdefiniowane w załączniku do ustawy.

j) Podsektor transportu wodnego ma obejmować: armatorów w transporcie morskim pasażerów i towarów, armatorów śródlądowego transportu pasażerów i towarów, podmioty zarządzające portami, podmioty zarządzające obiektami portowymi, podmioty prowadzące na terenie portu działalność wspomagającą transport morski oraz operatorów systemów ruchu statków. Załącznik odwołuje się do definicji rozporządzenia (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych, armatorów żeglugi śródlądowej – ustawa z dnia 21 grudnia 2000 r. o żegludze śródlądowej, ustawa z dnia 20 grudnia 1996 r. o portach i przystaniach morskich, ustawa z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim.

k) Podsektor transportu drogowego: regulacją mają być objęte organy administracji drogowej oraz operatorzy inteligentnych systemów transportowych. W polskim systemie prawnym sektor transportu drogowego reguluje ustawa o drogach publicznych.

l) Zgodnie z dyspozycjami dyrektywy 2016/1148 regulacja krajowa ma w załączniku obejmować instytucje kredytowe objęte rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 575/2013 w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych. W polskim systemie prawa regulacje dotyczące instytucji kredytowych znajdują się w ustawie – Prawo bankowe i w ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych. Załącznik odwołuje się tutaj do art. 4 ust. 1 pkt 17 ustawy – Prawo bankowe oraz do definicji banku krajowego (art. 4 ust. 1

pkt 1 Prawa bankowego), oddziału banku zagranicznego (art. 4 ust. 1 pkt 20 ustawy – Prawo bankowe), oddziału instytucji kredytowej (art. 4 ust. 1 pkt 18 ustawy – Prawo bankowe). Zakresem załącznika niniejszej ustawy będzie również objęty sektor spółdzielczych kas oszczędnościowo-kredytowych, objęty ustawą o spółdzielczych kasach oszczędnościowo-kredytowych.

ł) W zakresie infrastruktury rynków finansowych załącznik do ustawy zgodnie z dyrektywą 2016/1148 odwołuje się do operatorów systemu obrotu i kontrahentów centralnych. Omawiany sektor jest regulowany w polskim systemie prawa przez ustawę o obrocie instrumentami finansowymi. Załącznik do ustawy odwołuje się tutaj do podmiotu prowadzącego rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy o obrocie instrumentami finansowymi (giełdy towarowej lub pieniężnej), obejmuje podmiot wskazany w art. 3 pkt 49 ustawy o obrocie instrumentami finansowymi, czyli Krajową Izbę Rozliczeniową SA., podmiot, o którym mowa w art. 48 ust. 7 ustawy o obrocie instrumentami finansowymi, czyli kontrahent centralny „CCP".

m) Zgodnie z wymogami dyrektywy 2016/1148 w załączniku zostały wskazane podmioty lecznicze, o których mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej. Dodatkowo ze względu na istotność usług i ich zależność od systemów informacyjnych, w porozumieniu z ministrem właściwym do spraw zdrowia ustalono dodatkowe kategorie podmiotów wykraczające poza zakres podmiotowy dyrektywy 2016/1148, z których będą mogli być wyłaniani operatorzy usług kluczowych. Będzie to jednostka podległa ministrowi właściwemu do spraw zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia, Narodowy Fundusz Zdrowia (NFZ), działy farmacji szpitalnej i apteki, hurtownie farmaceutyczne, przedsiębiorcy, którzy wnioskują lub uzyskali pozwolenie na dopuszczenie do obrotu produktu leczniczego, wytwórcy, importerzy produktu leczniczego/substancji czynnej i dystrybutorzy substancji czynnej oraz importerzy równolegli.

n) Regulacja w załączniku ma obejmować dostawców i dystrybutorów „wody przeznaczonej do spożycia przez ludzi". Sektor ten uregulowany jest w polskim systemie prawnym w ustawie z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków. W ustawie tej znajduje się definicja przedsiębiorstwa wodno-kanalizacyjnego, który może zostać uznany za operatora usługi kluczowej.

o) Regulacja w załączniku ma obejmować podmioty prowadzące punkty wymiany ruchu internetowego (IXP), stanowiące obiekt sieciowy, który umożliwia połączenie międzysystemowe między więcej niż dwoma niezależnymi systemami autonomicznymi, podmioty świadczące usługi autorytatywnych serwerów DNS, podmioty zarządzające rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD).

[841] Jeżeli chodzi o jednostki sektora finansów publicznych, to zostały one zawężone do tych określonych w art. 9 pkt 1–6, 8–9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (dalej ustawa o finansach publicznych).

Są to trzy grupy podmiotów, które w opinii projektodawcy wymagają szczególnej uwagi w zakresie uregulowania kwestii związanych z cyberbezpieczeństwem. Do pierwszej grupy zaliczono organy władzy publicznej. Do drugiej grupy należą ZUS (w tym FUS) i KRUS (w tym jej fundusze). Do trzeciej grupy należą uczelnie publiczne oraz PAN i jego jednostki organizacyjne organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały, jednostki samorządu terytorialnego oraz ich związki (w tym metropolitarne), jednostki budżetowe i samorządowe zakłady budżetowe, agencje wykonawcze oraz instytucje gospodarki budżetowej.

[842] http://www.cyberdefence24.pl/625839,niemiecka-agencja-cyberbezpieczenstwa-powazne-skutki-ataku-hakerow (dostęp: 07.07.2020).

[843] Ibidem.

[844] *Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen,* Bundesministerium des Innern, Berlin 2007, s. 10.

[845] *Cyber Security Strategy for Germany*, Bundesministerium des Innern, Berlin 2011, s. 11 i n.

[846] *Nationale Strategie zum Schutz Kritischer Infrastrukturen,* Bundesministerium des Innern, Berlin 2009, s. 5–6.

[847] Ibidem, s. 10–13.

[848] *Cyber Security Strategy for Germany*, s. 4–6.

[849] www.coe.int/cybercrime (dostęp: 11.07.2017).

[850] Konwencja Rady Europy o cyberprzestępczości sporządzona w Budapeszcie 23 listopada 2001 r. (Dz.U. z 2015 r. poz. 728).

[851] I. Oleksiewicz K. Michalski, E. Sienkiewicz, *Bezpieczeństwo w społeczeństwie informacyjnym. Zagadnienia w wymiarze online i offline*, Warszawa 2017, s. 45.

[852] *Cyber-Sicherheitsstrategie für Deutschland 2016*, Bundesministerium des Innern, Berlin 2016, s. 4–9.

[853] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBI. I S. 1324).

[854] Ustawodawca przewidział możliwość samoregulacji: operatorzy lub związki gospodarcze danego sektora będą mogły wypracować własne standardy w zakresie minimum wymagań bezpieczeństwa IT i wnioskować do Federalnego Urzędu Bezpieczeństwa Teleinformatycznego (Bundesamt für Sicherheit in der Informationstechnik – BSI) o ich uznanie.

[855] Skutecznie zainfekowany komputer łączy się z serwerem i czeka na polecenia od cyberprzestępcy. Wiele zainfekowanych w ten sposób komputerów, kontrolowanych przez jednego przestępcę lub grupę, nazywamy botnetami, http://di.com.pl (dostęp: 7.07.2017).

[856] Odbywa się to w myśl pkt 30 art. 3 ustawy telekomunikacyjnej (TKG). Mogą być gromadzone, przetwarzane lub wykorzystywane do świadczenia usługi telekomunikacyjnej.

[857] Telekommunikationsgesetz vom 22.06.2004 (BGBI, I s.1963).

[858] *Germany passes strict cyber-security law to protect „critical infrastructure”*, https://www.rt.com/news/273058-german-cyber-security-law/ (dostęp: 07.07.2017).
[859] *Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg,* 2015, https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/#Strategische-Leitlinie-Cyber-Verteidigung (dostęp: 7.07.2017).
[860] Strafgesetzbuch (StGB) vom 15.05.1871 (BGBI, I s. 3083).
[861] Urheberrechtsgesetz (UrhG) vom 09.09.1965 (BGBI, I s. 3037).
[862] Szerzej: http://www.coe.int/cybercrime (dostęp: 11.07.2017).
[863] M. Siwicki, *Pojęcie locus delicti i zasady jurysdykcji karnej w ujęci prawnoporównawczym* (cz. I), „Europejski Przegląd Sądowy” 2011, nr 9, s. 25.
[864] Ibidem, s. 28.
[865] U. Sieber, *Cybercrime and Jurisdiction in Germany. The Present Situation and the Need for New Solutions*, w: B.J. Koops, S.W. Brenner (red.), *Cybercrime and Jurisdiction. A global survey*, „Information Technology & Law Series” 2006, t. 11, s. 188.
[866] Strafgesetzbuch (StGB) vom 15.05.1871 (BGBI, I s. 3083).
[867] Konwencja z 2001 r. nazywa to bezprawnym dostępem do danych (art. 2).
[868] W konwencji jest to naruszenie integralności danych.
[869] W myśl art. 115 § 14 k.k. dokumentem w rozumieniu kodeksu karnego jest każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne.
[870] Wyrok SN z 3.06.1996 r., sygn. akt II KKN 24/96, „Prokuratura i Prawo” 1997, nr 2, poz. 5.
[871] Por.: A. Wąsek, R. Zawłocki (red.), *Kodeks karny. Część szczególna*, s. 760–765.
[872] Wyrok SN z 26.10.1938 r., sygn. akt 1 K 2813/37 (OSN(C) 1939, nr 6, poz. 135).
[873] Szerzej: http://www.coe.int/cybercrime (dostęp: 11.07.2017).
[874] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009 (BGBl. I S. 2821).
[875] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5 (dostęp: 11.07.2017).
[876] Raport BSI demonstruje nową jakość zagrożenia, którą jest rosnąca digitalizacja i sieci w wyniku rozwoju Internetu i Przemysłu 4.0 lub inteligentnych możliwości szpiegowania informacji, procesów biznesowych i administracyjnych sabotaży. Napastnicy mają wydajne i elastyczne środki oraz metody ataku, dlatego odkryli dziennie 380 tys. nowych wariantów szkodliwego oprogramowania, ilość spamu ze złośliwym oprogramowaniem wzrosła o 1,270%. Jednocześnie poprzednie klasyczne środki obronne nadal tracą swoją skuteczność. Głównym celem ataków są firmy i infrastruktura krytyczna,

administracja publiczna, instytucje badawcze i obywatele. Ataki *ransomware* wiosną 2016 r. uwidoczniły konsekwencje tych zmian oraz podatność na cyberzagrożenia społeczeństwa informacyjnego, https://www.bsi.bund.de (dostęp: 11.07.2017).

[877] Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG) vom 20 Dezember 1990 (BGBI. s. 2576). Zgodnie z § 3 BVerfSchG zadaniem urzędów ds. ochrony konstytucji na szczeblu zarówno krajowym, jak i lokalnym jest gromadzenie i analiza informacji, zwłaszcza rzeczowych i osobowych, nowości i dokumentacji o:

– zwalczaniu demokratycznego porządku prawnego w RFN,
– istnieniu niebezpieczeństwa federalnych lub stanowych organów ds. ochrony konstytucji,
– naruszeniu bezpieczeństwa państwa lub działalności wywiadu w zakresie tej ustawy,
– istnieniu niebezpieczeństwa w szczególności w stosunku do pokojowego współistnienia narodów (art. 26 ust. 1 Konstytucji).

[878] Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (Zivilschutz- und Katastrophenhilfegesetz – ZSKG) vom 25.03.1997 (BGBl. I S. 726).

[879] Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt z 25.12.2008 r. BGBI. I, s. 3083).

[880] Gesetz über den Bundesnachrichtendienst (BND – Gesetz – BNDG) vom 20 Dezember 1990 (BGBI. S. 2576).

[881] Ibidem.

[882] Gesetz über die Bundespolizei (Bundespolizeigesetz – BPolG) vom 19. Oktober 1994 (BGBl. I S. 2978, 2979).

[883] K. Sacewicz, *Niemiecka strategia ochrony cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, vol. 7, s. 132.

[884] Szerzej: I. Oleksiewicz, *Polityka antyterrorystyczna*, s. 423.

[885] Szerzej: Raport RFN dla ONZ, dok. S/AC.37/2003/(1455)/10.

[886] I. Oleksiewicz, *Polityka antyterrorystyczna*, s. 436.

[887] Überblick: Cyber-Abwehr der Bundeswehr, http://www.bmvg.de/ *(*dostęp: 7.07.2017).

[888] cirbw.de umziehen (dostęp: 7.07.2017).

[889] https://www.bundeswehr.de (dostęp: 11.07.2017).

[890] http://www.kooperationssysteme.de/2013/04/05/forschungszentrum-cyber-operations-defence-code/lang-pref/de/ (dostęp: 11.07.2017).

[891] Défense et Sècurité nationale. Le Livre Blanc, 2008, http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/livre_blanc_tome1_partie1.pdf (dostęp: 30.07.2020).

[892] M. Kamiński, J. Strużewska-Smirnow, M. Wieczerza, *Charakterystyka modeli systemów bezpieczeństwa teleinformatycznego oraz ochrony sieci teleinformatycznych z punktu widzenia służb specjalnych*, w: P. Pogonowski (red.), *Charakterystyka modeli systemów bezpieczeństwa teleinformatycznego oraz ochrony sieci teleinformatycznych z punktu widzenia służb specjalnych*, Warszawa 2017, s. 120.

[893] *Décret n° 2009-834 du 7 juillet 2009 portant creation d'un service à competence nationale dénommé*.

[894] Défense et sécurité des systèmes d'information. Stratégie de la France, https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-0215_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf (dostęp: 30.07.2020).

[895] Por.: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 227.

[896] Por. uwagi zawarte na ten temat w raporcie *La cyber résilience* z 2018 r. https://www.economie.gouv.fr/files/files/directions_services/cge/Rapports/2017_02_CGE_SR_Rapport.pdf (dostęp: 30.07.2020).

[897] Informacje mające największe znaczenie strategiczne zostały określone w dokumencie jako informacje istotne dla zachowania suwerenności, których prawidłowa ochrona jest warunkiem zachowania suwerenności i autonomii w polityce zarówno wewnętrznej, jak i zagranicznej.

[898] Défense et Sécurité nationale. Le Livre Blanc, 2013, www.livreblancdedefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf (dostęp: 30.08.2020).

[899] Pacte Défense Cyber – 50 mesures pour changer d'échelle, www.defense.gouv.fr/content/download/237708/2704474/file/Pacte%20D%C3%A9fense%Cyber-1.pdf (dostęp: 30.07.2020).

[900] Szerzej: M. Kamiński, J. Strużewska-Smirnow, M. Wieczerza, *Charakterystyka modeli*, s. 124–125.

[901] https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/ (dostęp: 30.07.2020).

[902] Por.: P. Mickiewicz, *System bezpieczeństwa narodowego*, s. 68.

[903] https://www.irsem.fr/data/files/irsem/documents/document/file/105/20170707-NP-CICDE-DIA-3.0.3-ASI-2017.pdf (dostęp: 30.07.2020).

[904] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portent diverses dispositions concernant la défense et la sécurité nationale.

[905] Loi n ° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[906] Loi n°2012-410 du 27 mars 2012 relative à Code penal.

[907] Loi n° 2015-912 du 24 juillet relative au renseignement, www.legifrance.gouv.fr/affichTexte.do?cid-Texte=JORFTEXT000030931899&categorieLien=id (dostęp: 30.07. 2020).
[908] Code de la sécurité intérieure (JO du 31/07/2020 version consolidée).
[909] Szerzej: J. Strużewska-Smirnow, M. Wieczerza, *Ustawowe uprawnienia operacyjno-rozpoznawcze i dochodzeniowo-śledcze służb specjalnych w zakresie wykrywania zagrożeń bezpieczeństwa narodowego w systemach i sieciach teleinformatycznych z perspektywy międzynarodowej*, w: P. Pogonowski (red.), *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego: wybrane zagadnienia*, Warszawa 2017, s. 171–172.
[910] Szerzej: M. Bohaczewski, *Jurysdykcja krajowa w sprawie o naruszenie praw własności intelektualnej w internecie na tle orzecznictwa francuskiego*, w: A. Sztoldman (red.), *Prawo wobec innowacji technologicznych*, Warszawa 2013, s. 46–50.
[911] Orzeczenie Sądu Okręgowego w Paryżu z 20 października 2000 r. w sprawie Anit-Semitism LICRA v. Yahoo! Inc., sygn. akt No RG 00/05308. 200.
[912] Wyrok Yahoo! v. La Ligue Contre le Racisme et l'Antisémitisme, sygn. akt 2006 WL 60670 (9th Cir. 2006) C-00-21275 JF.
[913] J. Kulesza, *Międzynarodowe prawo Internetu*, Poznań 2010, s. 107.
[914] Wyrok Cour d'appel w Paryżu z 27.09.2006 r., nr 04-20185.
[915] Stan faktyczny odnosił się do 2001 r.
[916] Por.: wyrok Sądu Kasacyjnego we Francji z 9.12.2003 r., *Cour de cassation* nr 01-03225.
[917] Por.: wyrok ETS z 25.10.2011 r. w sprawie eDate Advertising v. Marines *(C-509/09*).
[918] Le décret núm. 2002–890 du 15 mai 2002 relatif au Conseil de sécurité intérieure.
[919] Le décret núm. 89–258 du 20 avril 1989, le CIR est chargé d'assurer l'orientation et la coordination des activités des services qui concourent au renseignement.
[920] Zob.: I. Oleksiewicz, *Polityka antyterrorystyczna*, s. 383.
[921] Zadaniem DST jest bezpośrednie przyczynianie się do zapobiegania i karania działalności terrorystycznej, wykorzystując swoje sądowe, administracyjne i policyjne uprawnienia do tego celu.
[922] DCRG zajmuje się niebezpiecznymi grupami terrorystycznymi.
[923] Por. też: *Codexter*, www.coe.int/gmt (dostęp: 30.04.2012).
[924] Ibidem.
[925] Por.: Ł. Wojciechowski, J. Trubalska (red.), *Bezpieczeństwo państwa w cyberprzestrzeni*, Lublin 2017, s. 130.
[926] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf (dostęp: 30.07.2020).

[927] Por.: A. Kozłowski, *Bezpieczeństwo cybernetyczne w strategicznych dokumentach Wielkiej Brytanii 2009––2011*, w: I. Panier (red.), *Wielka Brytania i Wspólnota u progu XXI wieku. Przeszłość – teraźniejszość – perspektywy*, Łódź 2014, s. 43–45.

[928] https://webarchive.nationalarchives.gov.uk/20121018134855/http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf (dostęp: 30.07.2020).

[929] https://www.gov.uk/government/publications/cyber-security-strategy (dostęp: 30.07.2020).

[930] Raport z realizacji cyberpolityki UK na lata 2011–2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf (dostęp: 30.07.2020).

[931] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (dostęp: 30.07.2020).

[932] Szerzej: *Raport z postępów działań w ramach cyberstrategii 2016–2021*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/805677/National_Cyber_Security_Strategy_Progress_Report.pdf (dostęp: 30.07.2020).

[933] *UK Public General Acts 1990* c. 18.

[934] Por. też: J. Strużewska-Smirnow, M. Wieczerza, *Ustawowe uprawnienia*, s. 212–214.

[935] Ibidem, s. 222.

[936] Wyrok ETPC z 29.03.2010 r. w sprawie n° 3394/03 (Medvedyev v. Francja); wyrok ETPC w sprawie z 15.11.1966 r. w sprawie Clauhal v. Wielka Brytania.

[937] Wyrok Sądu Apelacyjnego House of Lords z 10.04.1997 r. w sprawie R. v. Governor of Brixton Prison and another, ex parte Levin, sygn. akt. 4 All ER 350, All ER 289.

[938] Zob.: www.coe.int/terrorism (dostęp: 30.04.2012).

[939] The National Security strategy of the United Kingdom, 2009.

[940] K. Jałoszyński, *Współczesny wymiar*, s. 156.

[941] S. Karnouskos, *Stuxnet Worm Impact on Industrial Cyber–Physical System Security*, w: *37th Annual Conference of the IEEE Industrial Electronics Society*, Melbourne 2011.

[942] M. Manzano, *Cyberwarfare*, Singapur 2018, s. 53.

[943] K. Liedel, T. Serafin, *Otwarte źródła*, s. 98–101.

[944] Por. też: P. Mickiewicz, *System bezpieczeństwa narodowego*, s. 69.

[945] M. Pietraś, *Bezpieczeństwo międzynarodowe*, w: M. Pietraś (red.), *Międzynarodowe stosunki polityczne*, Lublin 2007, s. 160–165.

[946] I. Oleksiewicz, *Polska polityka antyterrorystyczna na tle standardów Unii Europejskiej*, „Przegląd Prawa Publicznego", Warszawa 2015, nr 6, s. 96–107.

[947] Por.: J. Gryz (red.), *Zarys teorii*, s. 127–128.

[948] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Zamknięcie obiegu – plan działania UE dotyczący gospodarki o obiegu zamkniętym, źródło: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52015DC0614, (dostęp: 12.07.2020).

[949] Szerzej: P. Zherestov, *From visible*, s. 55–67; K. Kjærgaard Christensen, T. Liebetrau, *A new role*, s. 399–400.

[950] R. Ottis, *Analysis of the 2007*, s. 25.

[951] „e-Terroryzm.pl" 2013, nr 5(17), s. 8.

[952] Ibidem, s. 21.

[953] M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 20.

[954] D. Verton, *Black ice*, s. 194.

[955] P. Maj, *Cyberterroryzm w stosunkach międzynarodowych*, http://www.politologia.pl/fck_pliki/File/consensus/consensus_1.pdf (dostęp: 15.12.2017). Por.: „e-Terroryzm.pl" 2013, nr 5(17) s. 10–12.

[956] Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Strategia Bezpieczeństwa Cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (JOIN(2013) 1 final, 7.02.2013).

[957] Ibidem.

[958] Dyrektywa Parlamentu Europejskiego i Rady UE nr 2016/1148 z dnia 6 lipca 2016 r. (Dz.Urz. UE L 194 z 19.07.2016).

[959] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE L 119 z 04.05.2016).

[960] Por.: *Raport TE-SAT 2018–19, European Union Terrorism Situation and Trend Report 2019–2019* (dostęp: 30.06.2020).

[961] *Biała Księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania* (COM(2020) 65 final.

[962] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz. Urz. UE., L 178, 17.07.2000).

[963] J. Black, A, Hall, K. Cox, M. Kepe, E. Silfversten, *Defence and security after Brexit. Understanding the possible implications of the UK's decision to leave the EU*, Santa Monica 2017, s. 37.

[964] Dz.Urz. UE L 316 z 25.10.2012.

[965] Ustawodawca zdefiniował cyberbezpieczeństwo jako odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne. Jest to definicja oparta na

definicji „bezpieczeństwa sieci i systemów informatycznych" wskazanej w dyrektywie 2016/1148, przy uwzględnieniu zmian niektórych pojęć. O ile problem ten prawnie uregulowano w Europie czy w Ameryce Płn., to np. Afryka czy Australia dopiero zaczynają stawiać pierwsze kroki regulacyjne w tym zakresie. Szczegóły przedstawiono na mapie na stronie internetowej www.coe.int. (dostęp: 30.06.2020).

[966] H. Carrapico, A. Barrinha, *The EU as coherent (cyber) security actor?*, „Journal of Common Market Studies" 2017, vol. 55(6), s. 1260–1261.

[967] Szerzej: I. Oleksiewicz, *Cyberbezpieczeństwo i sztuczna inteligencja w sektorze energetycznym UE, „*Rocznik Bezpieczeństwa Międzynarodowego" 2020, t. 13(1), s. 230–235.

[968] M. Paździor, J. Trubalska, *Pojęcie bezpieczeństwa państwa*, w: M. Paździor i in. (red.), *Bezpieczeństwo państwa w XXI wieku*, Lublin 2018, s. 15–20.

[969] H. Wyrębek, P. Szmitkowski, *Koncepcja*, s. 147–156.

[970] W. Krztoń, I. Oleksiewicz, *Bezpieczeństwo*, s. 30.

[971] Źródło: *Cyber Security Report 2020,* https://research.checkpoint.com (dostęp: 30.08.2020)

[972] Szerzej: L. Zacher, *Transformacje i perspektywy społeczeństw informacyjnych*, „Nierówności społeczne a wzrost gospodarczy", Rzeszów 2013, z. 32, s. 536–537.

[973] Szerzej: P. Sienkiewicz, *Prognozowanie rozwoju globalnego społeczeństwa informacyjnego: wizje i scenariusze*, w: A. Szewczyk, E. Kot (red.), *Fenomen Internetu*, Szczecin 2008, t. 1, s. 2.

[974] J. Golinowski, *Perspektywa porządku postpolitycznego. W stronę technologii władzy*, Warszawa 2007, s. 63.

[975] E. Polak, *Od „ciężkiej" do wirtualnej gospodarki*, „Transformacje" 2010, nr 1–2, s. 239–249.

[976] Por.: L.W. Zacher, *Odrealnienie człowieka i jego świata. Wstępne refleksje i uwagi*, w: A. Kiepas, M. Sułkowska, M. Wołek (red.), *Człowiek a światy wirtualne*, Katowice 2009, s. 145–152.

[977] J. Niżnik, *Socjologia wiedzy*, Warszawa 1979, s. 148.

[978] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne. Szanse, zagrożenia, wyzwania*, Warszawa 1999, s. 20–25.

[979] Por.: T. Galewski, *Transformacja społeczna w kierunku społeczeństwa informacyjnego: wizja czy rzeczywistość?*, „Zeszyty Naukowe Wyższej Szkoły Bankowej", Wrocław 2011, nr 22, s. 106–110.

[980] J. Janowski, *Cybernatyzacja*, s. 27.

[981] Dawny art. 249 TUE dotyczący hierarchii źródeł prawa wtórnego.

[982] Por.: art. 4 pkt 2 dyrektywy NIS i art. 2 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa.

[983] Por.: J. Gryz, *Zarys teorii*, s. 127–128.